

FAMILIES FIGHTING FOR JUSTICE CONSTITUTION

Date implemented 11th January 2010

Families Fighting for Justice and the O.L.L.Y Project objectives are to carry out activities which benefit the community and in particular (without Limitation) address the needs of parents, husbands, wives, partners, sisters, brothers, relatives and friends who have lost loved ones through the act of murder and violence.

1. Objects

1. To protect the health of and to relieve poverty, distress and suffering of persons who are or are likely to become victims of crime and the families of such persons.
2. To promote for the benefit of the public the provision of services for mediation and conciliation between victims of crime and offenders, with a view to the preservation of public order, and for the preservation and protection of the well-being of such victims and the rehabilitation of such offenders.
3. To advance education in the problems of criminal activity and its implications on society and the victims of crime and their families.

2. Powers

In furtherance of the objects but not otherwise, the society shall have the:

1. power to raise funds and to invite and receive contributions provided that in raising funds the Management Committee shall conform to any relevant requirements of the law;
2. power to buy, take on lease or in exchange any property necessary for the achievement of the objects and to maintain and equip it for use;
3. power subject to any consents required by law to sell, lease or dispose of all or any part of the property of the Charity;
4. power subject to any consents required by law to borrow money and to charge all or any part of the property of the Charity with repayment of the money so borrowed;
5. power to employ such staff as are necessary for the proper pursuit of the object and to make all reasonable and necessary provision for the payment of pensions and superannuation for staff and their dependents; Section 185 of the Charity Act 2011 a Trustee or a Management Committee member can be paid where they provide services to the charity that are distinct from their role as Trustee or Management member.
6. power to co-operate with other charities, voluntary bodies and statutory authorities operating in furtherance of the objects or of similar charitable purposes and to exchange information and advice with them;
7. power to establish or support any charitable trusts, associations or institutions formed for all or any of the objects;
8. power to appoint and constitute such committees as the Management Committee may think fit;
9. power to engage in political activity provided that the Management Committee are satisfied

that the proposed activities will further the purposes of the charity to an extent justified by the resources committed and the activity is not the dominant means by which the charity carried out its objects.

10. Power to do all such other lawful things as is necessary for the achievement of the objects.

3. Membership

1. Membership of the charity shall be open to any person over 18 interested in and committed to furthering the works of the charity and who have their application approved by the Management Committee.
2. The first members shall be accepted to full membership at the first meeting of the Management Committee, where this constitution shall be first adopted.
3. Any subsequent individuals gaining entry to membership shall be granted associate member status.
4. Associate members shall become eligible for full membership status after a six-month period, subject to approval by the Management Committee.
5. The Management Committee may from time to time define additional categories of membership, as well as the rights and obligations associated with such membership, subject to clause 3. 6.
6. Every full member shall have one vote. Associate members or any other category of member defined by the Management Committee shall have no voting rights within the organization.
7. The Management Committee may unanimously and for good reason terminate the membership of any individual, provided that the individual concerned or the appointed representative of the member organization concerned (as the case may be) shall have the right to be heard by the Management Committee, accompanied by a friend, before a final decision is made.
8. The Management Committee must maintain a membership list, including the dates that individuals enter and leave each category of membership.

4. General Meetings.

1. Members are entitled to attend general meetings either personally or by proxy. Notice of intention to appoint a proxy must be delivered to the **Secretary** at least 24 hours before the meeting. Such notice should be in writing where possible. Any notice submitted in a manner other than in writing shall only be accepted upon its confirmation by at least 2 full members other than the nominating individual, the nominated proxy and members of the management committee.
2. General meetings are called on at least 14 days' notice specifying the business to be discussed, unless otherwise specified in the constitution. Notice may be in writing, in person, telephone, email or other suitable electronic means. Meetings other than the Annual General Meeting (AGM) may be called at shorter notice if all full members agree.
3. The first Annual General Meeting (AGM) shall be held no later than the last day of the 12th month following the date this constitution is first adopted. All subsequent AGMs shall be held no later than the last day of the 12th month following the date of the previous AGM. The membership shall receive at least 14 days notice of the date of the AGM.
4. The business of the AGM shall be to:
 - a) Receive the report of the Committee for the year just completed;
 - b) Approve the accounts of the organization for the year just completed;
 - c) Elect the Committee for the current year;
 - d) Approve any changes in level of subscriptions;
 - e) Discuss any other relevant business.
3. The quorum for general meetings shall be 12 or one tenth of the full, voting members, unless otherwise stated in the constitution. Only full members shall count towards the quorum.
4. The method of voting shall be decided by the Management Committee and shall be by simple majority of those present and voting, unless otherwise stated in the constitution. In the event of an equality of votes, the Chairperson shall casting vote.
5. A written resolution signed by those entitled to vote at a general meeting is as valid as a resolution actually passed at a general meeting. For this purpose the written resolution may be set out in more than one document and will be treated as passed on the date of the last signature required to pass the resolution in question.
6. The Management Committee may call a special general meeting of the Charity at any time. If at least four full members request such a meeting in writing stating the business to be considered the secretary shall call such a meeting. At least 14 days' notice must be given. The notice must state the business to be discussed.

5. Management Committee

1. The Management Committee will be elected at the first adoption of the constitution and at every AGM thereafter. All the members of the Management Committee shall retire from office together at the end of the AGM next after the date on which they came into office but they may be re-elected or re-appointed.
2. The Management Committee will consist of a minimum of 6 and maximum of 8 full members.
3. The proceedings of the Management Committee shall not be invalidated by any vacancy among their number or by any failure to appoint or any defect in the appointment or qualification of a member.
4. Nobody shall be appointed as a member of the Management Committee who is aged under 18.

5. The Management Committee shall choose from their own number the Chair, Secretary and Treasurer and any other honorary officers.
6. The Management Committee may in addition appoint co-opted members but so that no-one may be appointed as a co-opted member, if as a result, more than one third of the members of the Management Committee would be co-opted members. Each appointment of a co-opted member shall be made at a meeting of the Management Committee and shall take effect from the end of that meeting, unless the appointment is to fill a place which has not been vacated in which case the appointment shall run from the date when the post becomes vacant.
7. The Management Committee shall be entitled to delegate any or all of its powers, as it sees fit, to any committee set up by the Management Committee of its own members, or to any individual member of the Management Committee, or to any person employed by the project.
8. The Management Committee shall cause full and accurate financial accounts, minutes of proceedings, and reports of voting at meetings to be kept, and shall ensure that all these are available for inspection by project members at any reasonable time.
9. The Management Committee may have sufficient cause after having heard the views of the person concerned, dismiss an honorary officer by a majority vote at a correctly called quadrate meeting.

6. Meetings and Proceedings of the Management Committee

1. The Management Committee shall hold at least two meetings each year. A special meeting may be called at any time by the Chair or by any two members of the Management Committee upon not less than 7 days' notice being given to the other members of the Management Committee of the matters to be discussed.
2. The Chair shall act as Chair at meetings of the Management Committee. If the Chair is absent from any meeting, the members of the Management Committee present shall choose one of their number to be Chair of the meeting before any other business is transacted.
3. There shall be a quorum when at least four members of the Management Committee are present at a meeting.
4. Every matter shall be determined by a majority of votes of the members of the Management Committee present and voting on the question but in the case of equality of votes the Chair of the meeting shall have a second or casting vote.
5. The Management Committee shall keep minutes, in books kept for the purpose, of the proceedings at meetings of the Management Committee and any sub-committee and shall ensure that all these are available for inspection by members at any reasonable time.
6. The Management Committee may from time to time make and alter rules for the conduct of their business, the summoning and conduct of their meetings and custody of documents. No rule may be made which is inconsistent with this constitution.
7. The Management Committee may appoint one or more sub-committees consisting of two or more members of the Management Committee for the purpose of making any inquiry or supervising or performing any function or duty which in the opinion of the Management Committee would be more conveniently undertaken or carried out by a sub-committee, provided that all acts and proceeding of any such sub- committees shall be fully and promptly reported to the Management Committee.

7. Determination of membership of Management Committee

1. A member of the Management Committee shall cease to hold office if he/she:
 - a) Is disqualified from acting as a member of the Committee by virtue of section 72 of the Charities Acts 1993 (or any statutory re-enactment or modification of that provision);
 - b) Becomes incapable by reason of mental health issues, illness or injury of managing and administering her own affairs;
 - c) Is absent without the permission of the Committee from three consecutive Management Committee meetings and the Committee resolve that her office be vacated; or
 - d) Notifies the Committee in writing, via the Secretary, in writing, of their wish to resign (but only if at least 3 members of the Committee will remain in office when the notice of resignation is to take effect).

2. The Management Committee may after having heard the views of the person concerned, remove an honorary officer by a majority vote at a correctly called quadrate meeting.

8. Finance

1. Families Fighting for Justice Financial year shall run from 1st April to the 31st March.
2. The funds of the Charity, including all donations, contributions and bequests, shall be paid into an account operated by the Management Committee in the name of the Charity at such bank as the Management Committee shall from time to time decide. All cheques drawn on the account must be signed by at least two members of the Management Committee.
3. The funds belonging to the Charity shall be applied only in furthering the objects.

9. Property

1. Subject to the provisions of sub-clause (2) of this clause, the Management Committee shall cause the title to;
 - a) all land held by or in trust for the charity which is not vested in the Official Custodian for Charities; and
 - b) All investments held by or on behalf of the charity;

To be vested either in a corporation entitled to act as custodian trustee or in not less than three individuals appointed by them as holding trustees. Holding trustees may be removed by the Management Committee at their pleasure and shall act in accordance with the lawful directions of the Management Committee. Provided they act only in accordance with the lawful directions of the Management Committee, the holding trustees shall not be liable for the acts and defaults of its members.

2. If a corporation entitled to act as custodian trustee has not been appointed to hold the property of the charity, the Management Committee may permit any investments held by or in trust for the charity to be held in the name of a clearing bank, trust corporation or any stock broking company which is a member of the International Stock Exchange (or any subsidiary of any such stock broking company) as nominee for the Management Committee, and may pay such a nominee reasonable and proper remuneration for acting as such.

10. Accounts

The Management Committee shall comply with their obligations under the Charities Act 1993 (or any statutory re-enactment or modification of that Act) with regard to:

1. the keeping of accounting records for the Charity
2. the preparation of annual statements of accounts for the charity;
3. the auditing or independent examination of the statements of account of the Charity; and
4. The transmission of the statements of account of the Charity to the Charity Commission.

11. Annual Report

The Management Committee shall comply with their obligations under the Charities Act 1993 (or any statutory re-enactment or modification of that Act) with regard to the preparation of an annual report and its transmission to the Charity Commissioners.

12. Annual Returns

The Management Committee shall comply with their obligations under the Charities Act 1993 (or any statutory re-enactment or modification of that Act) with regard to the preparation of an annual return and its transmission to the Charity Commissioners.

13. Benefits to Members and Trustees

1. The property and funds of the charity must be used only for promoting the Objects and do not belong to the **members** but:
 - a) Members may enter into contracts with the charity and receive reasonable payment for goods or services supplied;
 - b) Members (including Trustees) may be paid interest at a reasonable rate on money lent to the charity;
 - c) Members (including Trustees) may be paid a reasonable rent or hiring fee for property or equipment let or hired to the charity; and
 - d) Members (including Trustees) who are also beneficiaries may receive charitable benefits, but **only** in that capacity.
2. A Trustee must not receive any payment of money or other **material benefit** (whether directly or indirectly) from the charity except:

as mentioned in clauses 13.1 b) (interest), 13.1 c) (rent), 13.1 d) (charitable benefits) or 13.3 (salaries and contractual payments); reimbursement of reasonable out-of-pocket expenses (including hotel and travel costs) actually incurred in the administration of the Group; an indemnity in respect of any liabilities properly incurred in running the Group (including the costs of a successful defence to criminal proceedings);

3. A Trustee may be an employee of the charity and may enter into a contract with the Group to supply goods or services in return for a payment or other material benefit, but only if:

- a) the goods or services are actually required by the charity;
- b) the nature and level of the benefit is no more than reasonable in relation to the value of the goods or services and is set at a meeting of the Management Committee in accordance with the procedure in clause 14; and
- c) No more than one third of the Trustees are contracted by the group at any one time.

14. Disclosure on Interests

1. Any trustee, member, or any person serving upon any of the Committees having or expectation to have any personal financial interest in any matter for consideration, shall declare that interest, shall take no part in any debate upon that matter unless providing information upon request and not vote or count towards the quorum for that part of the meeting. The declaration of that interest and of the member's abstention shall be recorded.

15. Alteration of the Constitution

1. Alterations to the constitution shall be proposed by decision of the Management Committee but shall require the approval of one third of the full, voting members. A resolution for the alteration of the Constitution shall be received by the Secretary at least twenty-one days before the meeting at which the resolution is to be brought forward. The Secretary shall give members at least fourteen days notice of such a meeting and shall include notice of the alterations being proposed.
2. No amendment may be made to the name of charity, clause 1 (objects), clause 13 (Benefits to Members and Trustees), clause 14 (Disclosure on Interests, clause 16 (Dissolution) or this clause without the prior consent in writing of the Charity Commission.
3. No amendment may be made which would have the effect of making the Charity cease to be a charity at law.
4. The Management Committee should promptly send to the Charity Commission a copy of any amendment made under this clause.

16. Dissolution

1. Dissolution of the charity shall be proposed by decision of the Management Committee but shall require the approval of one third of the full, voting members.
2. At least twenty-one days notice shall have been given to all full members of any proposed resolution.
3. Such resolution may give instructions for the disposal of any assets held or in the name of Families Fighting for Justice provided that if any property remains after the satisfaction of all debts and liabilities such property shall not be paid to or distributed among the members of Families Fighting for Justice, but shall be given or transferred to such other charitable institution or institutions (having objects similar to some or all of the objectives of the group.) as Families Fighting for Justice may with the approval of the Charity Commissioners or other authority having charitable jurisdiction, determine.
4. If the proposal is confirmed the Management Committee shall then have the power to realize any assets held by or on behalf of the Charity. Any assets remaining after the satisfaction of any proper debts and liabilities shall be given or transferred to such other charitable institution or institutions having objects similar to the objects of the Charity as the members of the

Charity may determine or failing that shall be applied for some other charitable purpose. A copy of the statement of accounts, or account and statement, for the final accounting period of the Charity must be sent to the Charity Commissioners.

17. Arrangements until First AGM

1. Until the first AGM takes place this constitution shall take effect as if references in it to the Management Committee were references to the persons whose signatures appear at the bottom of this document.
2. This constitution was adopted on the date mentioned above by the persons whose signatures appear at the bottom of this document.

Signed

G. Taylor

13.01.10

Chair

Secretary

Treasurer

A. Jones ANDREW JONES

J. Lyell JOAN LYELL

J. Hopley JUNE HOPLEY

R. Tyson REBECCA TYSON

M. Burns MARIE BURNS

Amended 11th November 2022

J. Langford

Jacqueline Langford

Jane C Williams

Jane Williams

The charity

Families Fighting for Justice (FFJ)

Families Fighting for Justice is a charity set up by our founder who lost a sister, son and daughter through separate acts of homicide. The charity was set up in 2008 and has been working tirelessly to support families who have lost a loved one through an act of murder, manslaughter or culpable road death. Families Fighting for Justice offers a drop-in centre, family bonding sessions, day trips and educational activities, trauma/bereavement counselling, group therapies, peer support, access to a Justice solicitor, court assistance, our re-building your future program and also, we explain the 28-day rule.

Families Fighting for Justice also delivers the Homicide Support HUB which is a one stop shop offering, information, guidance, advice and referrals onto relevant support which can be Families Fighting for Justice and OLLY (Our Lost Love Years) our children's group. Families Fighting for Justice is working in partnership with our Police and Crime Commissioner's Victim Care Merseyside.

O.L.L.Y (Our Lost Love Years)

O.L.L.Y was established in 2010 to provide targeted support to children and young people by engaging them in meaningful activities designed specifically to help them have fun, establish friendships, offer meaningful education and give them security and a sense of belonging, we do this through day trips out, art and craft sessions, annual camping trip, easter and Christmas drops to the homes of the children.

Following the loss of a family member a child or young person can feel isolated and forlorn and often unable to articulate their feelings, often causing them to become withdrawn or disruptive out of frustration or anger. This then becomes a barrier between them and the outside world as they try to make sense of what has happened and how it has affected them and their surviving family members. Children are often pushed aside not deliberately but mainly because the parent/carer is trying to deal with their own grief and often caught up in fighting for justice for the person they have lost

Families Fighting for Justice and O.L.L.Y

(Our Lost Love Years)

Confidentiality and Data Protection Guidelines

Reviewed: 1st March 2023

Most volunteer involving organisations hold information on their staff, volunteers and perhaps their clients. This information is likely to be personal data, and therefore subject to the 1998 Data Protection Act which gives rights to Data Subjects (the people whose data you have) and creates a framework of good practice for those holding personal data. If you collect and hold personal data on individuals, then you are legally required to comply with the Act.

What is the Data Protection Act?

The Data protection act 1998 regulates the collection, storage, use and disclosure of information about individuals by organisations. Any organisation that keeps information about individuals must comply with the act.

Data Protection Principles

Eight principles are defined to ensure that all 'personal data' is handled properly. The act states that the data must be:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

All employees paid/unpaid must conform in accordance with these principles.

Under S.51 (1) It shall be the duty of the commissioner to promote the following of good practice by data controllers and so to perform his functions under this Act as to promote the observance of the requirements of this Act by Data Controllers.

Under Schedule 5 (1) the corporation sole by the name of the Data Protection Registrar established by the Data Protection Act 1984 shall continue in existence by the name of (Information Commissioner).

Why is following these principles important?

Failure to observe these principles puts the professional reputation of your organisation at risk. Good information handling enhances your organisation's reputation by increasing member, customer and partner confidence in the organisation. Data protection is the responsibility of all members as well as all staff and agency or contract employees.

Reviewed 1st March 2023

CONFLICTS OF INTEREST

This policy is subject to the provisions of the Families Fighting for Justice constitution. Articles 13 and 14 will apply. Any amendment to articles 13/14 of the constitution will require amendment to this policy.

The relevant provisions of the constitution are repeated here for information and will apply where relevant.

Benefits to Members and Trustees

1) The property and funds of the charity must be used only for promoting the objects and do not belong to the members but:

- Members may enter contracts with the charity and receive reasonable payment for goods or services supplied.
- Members (including Trustees) may be paid interest at a reasonable rate or money lent to the charity.
- Members (including Trustees) may be paid a reasonable rent or hiring fee for property or equipment let or hired to the charity and;
- Members (including Trustees) who are also beneficiaries may receive charitable benefits, but **only** in that capacity.

2) A Trustee must not receive any payment of money or other material benefit (whether directly or indirectly) from the charity except:

As mentioned in clauses 13.1b) (interest), 13.1 c) (rent), 13.1d) (charitable benefits) or 13.3 (salaries and contractual payments); reimbursements of reasonable out of pocket expenses (including hotel and travel costs) actually incurred in the administration of the Group; an indemnity in respect of any liabilities properly incurred in running the Group (including the costs of a successful defence to criminal proceedings)

Examples of good practice

When Trustees become aware of a new actual or potential conflict of interest, they should give notice of it to the secretary to enable him/her to update the conflicts register.

The secretary should include in their report for each trustees' meeting details of any contracts/agreements to be entered into prior to the next meeting of the trustees and any potential conflicts identified from a check of the Register.

Competitive tendering for contracts or work for which a trustee might be suited (and taking up references from other clients or customers)

3) A trustee may be an employee of the charity and may enter a contract with the group to supply good or services in return for a payment or other material benefit, but only if:

a) The goods or services are required by the charity.

b) The nature and level of the benefit is no more reasonable in relation to the value of the goods or services and is set a meeting of the Management Committee in accordance with the procedure in clause 14 and

c) No more than one third of the Trustees are contracted by the group at any one time.

Disclosure on Interests

Any trustee, member, or any person upon any of the Committee having or expectation to have any personal financial interest in any matter for consideration, shall declare that interest shall take no part in any debate upon that matter unless providing information upon request and not vote or count towards the quorum for that part of the meeting. The declaration of that interest and of the member's abstention shall be recorded.

Further Policy statements

If a trustee has any other interest in a matter under discussion which creates a real danger of bias, that is, the interest affects they are or a member of their household more than the generality affected by the decision they should declare the nature of the interest, withdraw the vote and not count towards the quorum. They shall not remain in the room unless they have a dispensation to speak to provide information.

If a trustee has any other interest which does not create a real danger of bias, but which might reasonably cause other to think it could influence their decision they should declare the nature of the interest but remain in the room participate in the discussion and vote if they wish.

If in any doubt about the application of these rules they should consult with their chair.

It is recommended that a trustee's interest is listed in a register.

Conflicts of Interest Declaration Form

As a trustee you are required to act in the best interest of Families Fighting for Justice. However inevitably trustees have a wide range of interests in private, public and profession life and these interests might on occasions conflict (for example Director of supplier or Consultant to Charity)

We are obliged to review any possible conflicts when preparing our annual report to ask you to supply the following details.

- Has Families Fighting for Justice made any loans to you?
- Have you, or people connected with you through family, business or another charity an interest in a contract or transaction with Families Fighting for Justice.
- Have you or any person connected with you derived any pecuniary benefit or gain from Families Fighting for Justice?

Signed-----

Date-----

Name-----

Organisation Name O.L.L.Y (Our Lost Love Years)

Complaints Procedure

Reviewed 1st March 2023

Approved by: Trustee Committee Families Fighting for Justice and O.L.L.Y (Our Lost Love Years)

How we will treat your complaint

1.1 This organisation makes all reasonable efforts to make sure that the highest possible standards are maintained. When they are not, we encourage service users and partners to tell us so that, wherever possible, we can put matters right or make improvements for future service delivery.

1.2 We want to:

- a) Make it easy for you to raise your complaint.
- b) Ensure your complaints are listened to.
- c) Know how you would like us to resolve your complaint,
- d) Make sure your complaint is handled in a satisfactory manner.

How and where to complain.

2.1 If you are not satisfied with any aspect of our service, you can direct your concerns to the worker responsible for your service. If this does not provide a satisfactory resolution, the complaint will be heard by the board of trustees who will attempt to resolve the complaint.

2.2 Complaints can be made in the following way:

- a) **In writing** - marking the letter 'private and confidential' and addressing it to the Board of Trustee's, 6 Anson Street, Liverpool, L3 5NY
- b) **All complaints** must be reported in writing within 28 days of the alleged incidents being recognised by the complaint

How long will it take?

3.1 Our aim is to resolve your complaint straightaway. However, if we have been unable to resolve your complaint within fifteen working days, we will write* to you to:

- a) Explain why the complaint has not been resolved.
- b) Inform who is dealing with the complaint.
- c) Explain the time scale expected for resolving the complaint.
- d) Upon receiving the letter of complaint, you will receive a response from us within 7 days to acknowledge that your letter has been received

Restrictions

We will attempt to resolve all concerns relating to its activities. However, these are certain types of complaints that we cannot deal with, including the following.

- a) A mistake that has not caused financial loss material inconvenience or material distress.
 - b) Matters that have been (or are being) dealt with by a court or tribunal.
 - c) A grievance against us arising from the execution of our obligations under law or binding agreement.
-
- And contact you in the format which you choose and/is accessible to you.

Families Fighting For Justice

Children and Vulnerable Adults Safeguarding Policy

Reviewed 1st March 2023

Statement of Policy

We will endeavour to ensure that children and vulnerable adults are safeguarded from harm while they visit our properties or participate in our activities.

We will do this by:

1. Making sure our trustees, staff and volunteers are carefully selected.
2. Providing appropriate training in issues of child protection.
3. Taking all reasonable steps to ensure the health, safety and welfare of any child or vulnerable adult in contact with the organisation.
4. Not physically, emotionally, or sexually abusing any child or vulnerable adult in contact with the organisation.
5. Taking all reasonable steps to prevent anyone involved in the organisation or any persons working for us or member of the public from putting any child or vulnerable adult in a situation in which there is an unreasonable risk to their health and safety.
6. Taking all reasonable steps to prevent anyone involved in the organisation, persons working for us or member of the public from physically, emotionally, or sexually abusing any child or vulnerable adult.
7. Reporting to a designated officer any evidence or reasonable suspicion that a child or vulnerable adult has been physically, emotionally, or sexually abused in contact with the organisation.
8. Implementing this policy in conjunction with any health and safety guidelines already in place.

Definitions

Neglect: The actual or likely persistent or significant neglect of a child or vulnerable adult, or the failure to protect a child or vulnerable adult from exposure to any kind of danger, including cold or starvation, or persistent failure to carry out important aspects of care, resulting in the significant impairment of the child's or vulnerable adult's health or development.

Physical Injury: Actual or likely deliberate physical injury to a child or vulnerable adult, or wilful neglect failure to prevent physical injury or suffering to a child or vulnerable adult.

Sexual Abuse: Actual or likely sexual exploitation of a child or vulnerable adult. The involvement of children and adolescents in sexual activities they do not truly comprehend or to which they are unable to give informed consent.

Emotional Abuse: Actual or likely persistent or significant emotional ill treatment or rejection resulting in severe adverse effects on the emotional, physical and/or behavioural development of a child or vulnerable adult. All abuse involves some emotional ill treatment.

Children and Vulnerable Adults Safety and Welfare Guidelines

These guidelines apply to:

- Any situation involving children and young people up to age 18, whether accompanied by adults or not. The organisation also recognises that vulnerable people of any age will benefit from similar safeguards. Whenever the guidelines refer to vulnerable adults, this is taken to also include children.
- All staff, contractors and consultants working at the organisation's property or events.

General duties of all staff and volunteers regarding the safety and welfare of children and similarly vulnerable people:

- To take all reasonable steps to protect vulnerable adults from hazards;
- To take appropriate action if an accident occurs;
- To strictly observe the code of behaviour given here;
- To take all reasonable steps to prevent abuse of vulnerable adults in contact with the organisation;
- To report any incident or suspicion of abuse.

Admission Policy

Children and vulnerable adults are welcome at any location where the organisation conducts its activities. Where unaccompanied children or vulnerable adults are concerned, staff and volunteers need to exercise discretion, where practicable contact details, for unaccompanied vulnerable adults, should be obtained at the point of entry in case of accident.

The main factors to consider are:

- The nature of the site;
- Age and understanding.

It would be unwise for instance, to let a young child roam unsupervised on a site with lots of water features, tempting heights or hiding places. This may also be the case for certain vulnerable adults. If you are worried on that account, it is fully acceptable to refuse admission –in a friendly manner – but explain that they will be welcome another time if accompanied.

Age, maturity, or understanding can be hard to judge. How sensible they are matters more than a child's age. If only an older child accompanies a group of young children, it can help to ask, 'Who's in charge?'

Code of Behaviour for all staff and volunteers

People working with the organisation must always observe the following requirements where children, young people or similarly vulnerable people are concerned.

You should always:

- Uphold the spirit and specific provisions of the Statement of Policy and these guidelines.
- Do your best to behave in an open and friendly manner but avoid being over familiar in word or action.
- In so far as possible, avoid situations in which you are alone with children or similarly vulnerable people. If necessary, move to a place where you can both be seen by other colleagues or other adults.
- If a child is hurt or distressed, do your best to comfort or reassure them without compromising their dignity or doing anything to discredit your own behaviour.
- Try to avoid any physical contact or behaviour that could be unwelcome or misconstrued. Physical touch should only be in response to a child's need and should respect their age and individual stage of development.

It may be appropriate to hold a child's hand, to put a comforting arm around their shoulder or carry them - for instance, if they have fallen. However, you should first explain what you have in mind and ask directly if that is what they want. Otherwise, it may be unwelcome or misinterpreted.

- Where you have to rely on your own judgement, always treat the child's welfare as paramount.

You have a strict duty never to subject any child to any form of harm or abuse. Failure to honour this will be treated as gross misconduct. This means that that it is unacceptable for example:

- To distress a child by shouting at them or calling them derogatory names;
- To slap a child;
- To hold a child in such a way that it causes pain, or to shake them;
- To physically restrain a child except to protect them from harming themselves or others;
- To take part in horseplay or rough games;
- To allow or engage in appropriate touching of any kind;
- To do things of a personal nature for vulnerable adults that they can do for themselves or an accompanying adult can do for them; this includes going to the toilet with a child unless another adult is present;
- To allow or engage in sexually suggestive behaviour within a child's sight or hearing, or make suggestive remarks to or within earshot of a child;
- To give or show a child anything which could be construed as pornographic;
- To seek or agree to meet vulnerable adults anywhere beyond normal visitor areas or off the organisation's property without the full prior knowledge and agreement of their parents or guardians.

Support in exercising your best judgement.

If you witness or suspect abusive behaviour towards a child, you should use the procedural guidelines that follow. We all appreciate that this may call for fine judgement and even courage.

As long as you honour this Code of Behaviour and the other guidance given here, you will have the practical, moral and legal support of senior colleagues in any situation where you have to rely on

your own judgement. If you are in any doubt as to what to do then you should contact the designated officer who will be able to provide you with the necessary advice.

Guidelines: What to do in particular circumstances

1. Protecting vulnerable adults from hazards or rash behaviour

We recognise that it is impossible to ensure that no person ever comes to harm. However, you should also at all times be alert to potential dangers, taking swift appropriate action to ensure safety, for example, getting repairs done, new warning notices, altering barriers etc. 'Reasonable' and 'likely' are the operative terms here. **This means allowing for factors such as the following**, especially when children or vulnerable adults are unaccompanied by adults:-

- Children are usually smaller than adults. So, for example something set at a reasonable height for an adult may be dangerous for a child or above their sight line.
- Also children are usually less strong than adults, which may affect the design of doors or gates.
- Children are primed to explore or play games. This means that we have got to do our best to anticipate adventurous behaviour and assess the risks involved.
- Children and possibly vulnerable adults may have less experience or a lower degree of understanding as to what constitutes danger. They can be unaware or heedless of dangers you can clearly recognise. Even when aware of danger, they may act through bravado.

You have a duty to prevent young people from coming to harm through their own rash actions.

- You need to judge carefully how to intervene.
- Often the best course is to guide them into a safe course of action, rather than just telling them to stop what they're doing – and it is better to give positive rather than negative instructions (e.g. "Walk on the grass, please" instead of "Get off the wall"). Or it may work to distract them from something dangerous.
- If you must tell them to stop what they're doing, try to be clear and definite about it. It helps to take a deep breath before you say anything!
- Avoid being officious or challenging. You need to exert your authority, not 'prove' it.
- If, despite your efforts, a young person persists in jeopardising their own or other people's safety, get help if you can or consider asking them to leave the site.
- If they are in danger and you cannot persuade them away from it, you should treat this as an emergency and contact the emergency services.

Restraint: If you think it is necessary to restrain a child from doing something, try nonphysical approaches – e.g. by talking to them, by asking them not to move if they are injured, by standing in the way. If you do have to use physical restraint, it should be the minimum necessary for their safety. If they are in imminent danger, you might need to hold them by their clothing. Whatever the circumstances, physical restraint must be appropriate and reasonable. Otherwise, it may be regarded as assault.

Alcohol and Illegal Drugs: If there appears to be illegal drinking in or around one of our properties, or you see anyone apparently taking drugs, giving them to others or being given them:

- You should not try to stop them, but;
- You should notify the Police – and try to keep an eye that they do not otherwise endanger themselves. Police involvement does not mean necessarily that they will be charged with any offence, but it does alert the Police and should result in experienced handling of the situation.

You must also take all reasonable steps to ensure that no other member of staff, volunteer, or member of the public compromises the health and safety of any child in contact with the organisation. For example, someone might move a barrier that has been placed with vulnerable adults in mind or overlook the likelihood of vulnerable adults being at an event or suggesting an activity that is inherently risky.

- This means intervening directly to prevent this or reporting the situation to someone with more authority to intervene.
- In dealing with the person, bear in mind that the situation is more likely to arise through enthusiasm or thoughtlessness than wilful negligence.

2. What to do if an accident happens

- Depending on your judgement of the situation, go to the scene immediately if possible and/or contact the emergency services.
- With vulnerable adults it can be hard to tell whether they have been injured or whether an injury is serious. If you have any doubt about this, you should err on the side of caution and contact the emergency services. Even if a child is accompanied and you think an accident is not being treated seriously enough, get medical assistance on your own initiative if necessary.
- Normal accident recording and reporting procedure apply.

First Aid

- Unless there is a good reason, First Aid should not be administered without the permission of the child's parent, teacher or accompanying adult. **A child cannot give consent.** If the parent is not on site, get their phone number, if possible. However, if a child is alone and say, unconscious, the situation should be dealt with as for any other visitor.
- If at all possible, treatment should only be given by a trained First Aider or Appointed Person.
- Provided this does not put the child at risk, always try to administer First Aid within sight and sound of other adults.
- Always tell the child exactly what you are doing and why.
- Unless it is irrelevant, ask the child or vulnerable adult if they use medication (e.g. for asthma, diabetes and epilepsy) or have any allergies. Some people have allergic reactions to stings. Unless it is a first occurrence, a parent, teacher or accompanying adult should know of any such conditions.
- For minor injuries, it is all right to use a non fluffy cloth or sticking plaster, but you may not offer any medication, including antiseptics or pills of any kind. If you have any doubts about

helping someone to use their own medication, phone **National Health Service Direct on 0845 4647 or the emergency services.**

- Any treatment should be as little as necessary without threatening the individual's well being. **If a child or vulnerable adult comes to you for comfort** because of a minor accident or fright, it is perfectly in keeping with the Code of Behaviour to hold their hand or put your arm around them. Just make sure:
 - That you know about any injury and do nothing to make it worse.
 - That physical contact is what the individual wants, and the kind of contact between you is appropriate to their age and stage of development.
 - Do your best to stay in sight of other adults.

If a child or vulnerable adult needs a doctor or hospital, call the emergency services.

It is nearly always best to stay on site with them and wait for the ambulance. You should only take the risk of bringing in the individual yourself if the emergency services ask you to do so because of exceptional circumstances.

3. **What to do if a child/vulnerable adult is unattended or lost**

- If you see a child or vulnerable adult who seems unattended or who is definitely lost, introduce yourself, find out their name, and try to establish whom they are with and where they last saw them. Ask them to come with you to the reception point/main entrance/designated meeting place. Remember that the other person(s) will be looking for the individual too, so stay within obvious places. If you come across an individual who is definitely lost, try to keep them from getting distressed – perhaps by distracting them with something interesting or giving them a 'job' to do. Make sure to keep them in your sight, and if you must leave them, only pass them on to someone you can rely upon to look after them.
- If a child or vulnerable adult is reluctant to come with you, explain that you are going to look – but try to keep them in sight while you do so. Do not try to force them to come with you. If necessary, call for help or stay with them until they have been reunited with someone that the individual recognises and is willing to be with.

Contact with unaccompanied children/vulnerable adults.

Try to avoid situations where you are alone with children/vulnerable adults, especially anywhere you are unlikely to be seen or heard. This is as much to protect yourself from suspicion as to protect the individual.

If you cannot avoid being alone with a child or vulnerable adult, you should take prudent precautions:

- Try to move with the individual to a place where there are other people.
- Avoid unnecessary physical contact.
- If you do have to touch the individual, make sure to get their agreement beforehand and try not to be over-familiar.

- If whomever the individual is with has not been found after a reasonable time, you should notify the Police. You must judge how long to wait before doing this; it depends on the individual and the circumstances. (If the police have been notified, it is important also to let them know if a lost person has been reunited with whoever accompanied them.)
- If you find a child or vulnerable adult in distress, do your best to comfort and reassure them without compromising their dignity or privacy. Again, it may help to distract them while you take practical steps to help them but be careful that what you do is openly in their best interests.
- If you come across a lost person who does not speak English, they probably have been accompanied and other visitors may be able to help find whoever that is.

Key details if reporting a lost child/vulnerable adult:

- **Name**
- **Age**
- **Accompanying person's name**
- **Address or name of school/group**
- **Physical description of the individual (height, colour of hair, distinctive clothing)**
- **Where the individual is now**
- **Where and when the individual was last seen**

4. What to do if someone is being violent to a child/vulnerable adult

If you come across someone hitting, hurting, or violently shouting at a child or vulnerable adult, you should try to prevent the abuse, if you can do so without unreasonable risk to the child/vulnerable adult or yourself.

- You have to judge whether it is a fleeting incident, which warrants showing your disapproval or a threat of actual harm that requires someone to intervene.
- You also have to judge whether intervening is likely to stop the abuse or to inflame the situation. This can be even more complicated if one child/vulnerable adult is being abused by another.
- So long as you are mindful of the individual's welfare, you are entitled to intervene by:
 - Asking or telling the perpetrator to stop
 - Explaining that such behaviour is not acceptable on the organisation's property or at its event
 - Restraining a child/vulnerable adult from abusing another
 - Saying that you will report the incident – as a matter of fact, not a threat
 - Summoning help
 - Notifying the National Society for the Prevention of Cruelty to Children (NSPCC) or the police
 - Asking the perpetrator to leave the property
- While you have to be firm, it can only help if you are calm and un-antagonistic. Bear in mind that you may be dealing with an upset or angry adult as well as a distressed child.

- Never use or threaten physical force as this could inflame the situation and result in further violence.
- If you have any doubt about what to do, consult the Designated Officers or one of the following:
 - 24 hour NSPCC Protection Helpline;
 - The local Social Services, there is normally a duty social worker available at all times.
- If you are worried about any incident, you should record the details and report it to the Designated Officer.

The same principles apply if there is a 'flasher' on site or someone behaving suspiciously towards children/vulnerable adults.

5. If you suspect a colleague or receive an allegation of abuse

We hope that you will never encounter any situation of abuse while you are with the organisation. However, you must know what to do if you discover an incident of abuse, suspect a colleague of abuse, or receive an allegation of abuse.

If you suspect a colleague

It is your duty to report your suspicions to the designated officer. **It is not your responsibility to investigate your suspicions.** Nor should you concern yourself with looking for evidence of abuse. This requires expertise you are not expected to have; your role is to respond appropriately.

If an allegation is made to you about a colleague

It is not your responsibility to investigate any allegation. Nor should you concern yourself with looking for evidence of abuse. This requires expertise you are not expected to have. Your role is to respond appropriately and to report what you have been told to the designated officer.

If a child/vulnerable adult makes a disclosure to you about abuse not involving organisation staff or volunteers.

It is not your responsibility to investigate any disclosure. Nor should you concern yourself with looking for evidence of abuse. This requires expertise you are not expected to have. **Your role is to respond appropriately and to report what you have been told to the NSPCC or local social services.** You should also inform the designated officer.

If a disclosure or allegation is being made to you:

- Listen carefully and sensitively, stay calm and offer understanding and reassurance.
- Check your understanding of the situation, without being investigative.
- Record what you have been told.
- Alert a senior colleague at the earliest opportunity within 24 hours.

Guidance on responding to a disclosure of abuse

DO YOUR BEST TO

- Stay calm
- Receive the information
- Listen, reassure
- Record the information
- Report to an appropriate colleague
- Accept your own feelings and consider getting support for yourself

DO NOT

- Probe in an investigative way or ask leading questions.
- Make a child/vulnerable adult repeat the story unnecessarily.
- Promise confidentiality.

If you become suspicious about the behaviour where children/vulnerable adults are concerned, of a colleague or someone associated with the organisation, steps 2, 3 and 4 above also apply.

If you think the situation is sufficiently seriously and urgent, contact the Designated Officer or, failing that the Police. Do not let anxiety that you might have jumped to a wrong conclusion deter you from reporting any genuine worries that you have. Procedures put in place will be used to follow up any such report, and we will not hold it against you should a well-intentioned, but mistake report be made.

If you feel you need expert support, because you come across abuse while working with us, we recommend that you discuss it with the designated officer.

6. If an allegation of abuse is made against you

- If an allegation is made directly to you, you should advise the Designated Officer, even if you think it is trivial.
- If we receive an allegation against you, we will inform you.
- All allegations of misconduct will be subject to standard disciplinary procedures.
- You are entitled to the moral and practical support if an unwarranted allegation of misconduct is made against you. If your behaviour is in line with the policy and these guidelines, we cannot envisage any allegation of misconduct being justified.
- Any allegation will be scrupulously investigated, with due regard for confidentiality.
- This should not be interpreted as indicating culpability. It is part of our duty to protect people working with us from any unfounded allegation.
- If your behaviour contravenes this policy and guidelines, it will be treated as gross misconduct.
- If you have concerns about how an allegation against yourself or anyone else is being dealt with, you should inform a colleague at the most senior level you think appropriate.

Supporting the Policy

Confidentiality

We recognise that it is important for us all to feel that any information about alleged or actual abuse will only be disclosed where it is in best interests of the child/vulnerable adult to do so. Furthermore, we have a responsibility to protect the identity of anyone reporting suspected or actual abuse. No such disclosure will be made without careful consideration.

The role of the designated officer

The nominated child and vulnerable adult protection officer(s) is (are):

Their role is twofold: to serve as a centre for information and guidance on child welfare issues, and to support trustees, staff, and volunteers in dealing with any suggestion of misconduct or need for expert advice (see Appendix A).

Disseminating information about this policy

- Everyone working or applying to work for us is to be made aware of our policy for children and vulnerable adult's welfare. Furthermore, these guidelines are being issues to all trustees, volunteers, staff, and other people who are likely to have contact with children as part of their work with us.
- Queries or suggestions regarding the policy or guidelines should be channelled through the designated officer.

Appendix A: The Role of the Designated Officer

The Child and Vulnerable Adult Protection Policy must include the name(s) of the Designated Officer(s), her/his role, and responsibilities and how s/he can be contacted.

The Designated Officer(s) should ensure that they are knowledgeable about child protection and that they undertake any training considered necessary to keep updated on new developments.

The Designated Officer(s) is the link between the members of the public, staff and statutory agencies. They will take responsibility for monitoring and reporting to the Board on how the policy impacts on vulnerable adults and organisation staff/volunteers.

The Designated Officer(s) will have the following functions:

- To promote awareness of the child/vulnerable adult protection policy within the organisation;
- To influence policy within the organisation in order to prioritise the needs of children and vulnerable adults;
- To be an advisor on best practice in regard to the child/vulnerable adult protection policy;
- To advise on and co-ordinate training for others, as appropriate;

- To build a network with relevant personnel in the Statutory Authorities;
- To agree incident reporting procedures;
- To keep records of incidents and reports, together with any other relevant information;
- To report incidents to the Statutory Authorities and ensure that appropriate information is available at the time of referral and that the referral is confirmed in writing, under confidential cover;
- To ensure that individual case records are maintained of the action taken by the organisation.

The Designated Officer does not have the responsibility of investigating or validating protection concerns within the organisation and has no counselling or therapeutic role.

Appendix B: Referral Contact List

- National Society for the Prevention of Cruelty to Children (NSPCC) 24 Hours Protection Helpline: 0808 800 5000
- Liverpool Social Services:
0151 233 3700 for Careline Children's Service
0151 233 3800 for Careline Adult Services (for all queries about people aged 18 and over)

If you are deaf or hard of hearing you can use the Minicom – 0151 225 2500

Families Fighting for Justice

Equal Opportunities Policy

Statement of Policy

1. Families fighting for justice recognise that discrimination is unacceptable and although equality of opportunity has been a long-standing feature of our employment practices and procedure, we have made the decision to adopt a formal equal opportunities policy. Breaches of the policy will lead to disciplinary proceedings and, if appropriate, disciplinary action.
2. The aim of the policy is to ensure no job applicant, employee or worker is discriminated against either directly or indirectly on the grounds of race, colour, ethnic or national origin, religious belief, political opinion or affiliation, sex, marital status, sexual orientation, gender reassignment, age or disability.
3. Families fighting for justice will ensure that the policy is circulated to any agencies responsible for our recruitment and a copy of the policy will be made available for all employees and made known to all applicants for employment.
4. The policy will be communicated to all private contractors reminding them of their responsibilities towards the equality of opportunity.
5. The policy will be implemented in accordance with the appropriate statutory requirements and full account will be taken of all available guidance and in particular any relevant codes of practice.
6. Families fighting for justice will maintain a neutral working environment in which no employee or worker feels under threat or intimidated.

Recruitment and Selection

1. The recruitment and selection process is crucially important to any equal opportunities policy. Families fighting for justice will endeavour through appropriate training to ensure that employees making selection and recruitment decisions will not discriminate, whether consciously or unconsciously, in making these decisions.
2. Promotion and advancement will be made on merit and all decision relating to this will be made within the overall framework and principles of this policy.
3. Job descriptions, where used, will be revised to ensure that they are in line with our equal opportunities policy. Job requirements will be reflected accurately in any personnel specifications.
4. Families fighting for justice will adopt a consistent, non-discriminatory approach to the advertising of vacancies.
5. Families fighting for justice will not confine our recruitment to areas or media sources which provide only, or mainly, applicants of a particular group.
6. All applicants who apply for jobs with Families Fighting for Justice will receive fair treatment and will be considered solely on their ability to do the job.

7. All employees involved in the recruitment process will periodically review their selection criteria to ensure that they are related to the job requirements and do not unlawfully discriminate.
8. Short listing and interviewing will be carried out by more than one person where possible.
9. Interview questions will be related to the requirements of the job and will not be of a discriminatory nature.
10. Families Fighting for Justice will not disqualify any applicant because he/she is unable to complete an application form unassisted unless personal completion of the form is a valid test of the standard of English required for the safe and effective performance of the job.
11. Selection decisions will not be influenced by any perceived prejudices of other staff.

Training and Promotion

1. Senior staff will receive training in the application of this policy to ensure that they are aware of its contents and provisions.
2. All promotion will be in line with this policy.

Monitoring

1. Families Fighting for Justice will maintain and review the employment records of all employees in order to monitor the progress of this policy.
2. Monitoring may involve:
 - The collection and classification of information regarding the race in terms of ethnic/national origin and sex of all applicants and current employees;
 - The examination by ethnic/national origin and sex of the distribution of employees and the success rate of the applicants; and
 - Recording equipment, training and promotional records of all employees, the decisions reached and the reasons for those decisions.
3. The result of any monitoring procedure will be reviewed at regular intervals to assess the effectiveness of the implementation of this policy. Consideration will be given, if necessary, to adjusting this policy to afford greater equality or opportunities to all applicants and staff.
- 4.

Families Fighting for Justice – Complaints Policy

If you have a complaint, you should follow the Complaints Procedure as set out below:

Process

The aims of the policy are to resolve complaints as quickly, effectively and fairly as possible and maintain a positive working environment. With this in mind, it is advised that, as far as possible, the informal stage of the procedure be employed. (See complaints form).

If informal resolution fails, or if it is not appropriate to resolve the complaint informally, the individual, individual's line manager or (if not appropriate) the Centre Manager or Chair of the Board may at any time start the formal stage of the procedure.

The objective of the informal stage is to remedy the situation by encouraging and facilitating communication between the complainant and the respondent and, where appropriate, to allow the matter to be resolved locally by the line manager.

The formal stage involves the submission of a written complaint which is then dealt with by a confidential investigation and decision-making process.

The policy focuses on providing a mechanism for dealing with cases where the complainant or the respondent is a member of staff. If either holds a manager's position the Board takes overall responsibility for ensuring that the matter is resolved. If the complaint concerns a member (s) of the Board, the complainant can approach his/her line manager or another member of the Board Committee.

The Decision-Making Process

Where possible the decision-making panel should have a minimum of 2/3 members. The panel may comprise individuals from Board Committee, or an independent organisation.

In the event that the panel finds that there is no case to answer to or that action other than disciplinary action should be taken, it is the responsibility of the panel to identify what course of action should be taken.

- If the panel decides that disciplinary action should be taken, a disciplinary hearing will be convened in line with the Centre's disciplinary and grievance policy.
- In accordance with the appeal stage of the Disciplinary and Grievance policy, if the case is found to be proven and a sanction imposed, the respondent has the right of appeal.
- In line with the appeal procedure, a separate appeal panel must be convened. This should comprise a minimum number of 2/3 panel members.
- The outcome of the disciplinary hearing may be reviewed in the light of the appeal. The decision of the appeal panel is final.
- If following the investigation, it is decided that there is no case to answer; the complainant has the right to appeal via the grievance procedure.
- The grievance must be lodged in writing and a review undertaken in line with the procedure.
- If as a result of the review the original decision is confirmed, the matter is concluded and the procedure is at an end.
- If, as a result of the review the original decision is overturned, the matter is resolved via the disciplinary procedure.
- The panel must also consider whether in bringing the complaint there was any malicious or vexatious intent on the part of the complainant and decide upon the appropriate course of action.
- It should be noted that, if at any point in the procedure there is evidence of the misuse of the policy by any party, action up to and including disciplinary action will be taken.
- Following the conclusion of the procedure an assessment will be made of:
 - (1) The existing working arrangements so that they can be readjusted as necessary to accommodate the staff who will be working together in the future.

- (2) Any action necessary to prevent the recurrence of the complaint or behaviour of a similar nature. This will include looking at the need for training, additional support, supervision or monitoring.

Staff

Staff, if you have a complaint speak to your line manager, as they are best placed to respond. If you fail to receive a reasonable response either from your line manager (or in turn the manager), then as your contract of employment states, you can continue your grievance procedure by writing to the board.

Members/Visitors

If any member or visitor of the Families Fighting For Justice wishes to make a complaint they can state the nature of their complaint by:

- Writing to the manager:-
 - Jean Taylor
Families Fighting For Justice
6 Anson Street
Liverpool
L3 6NY
- Telephoning the manager on 0151 7092994
- Meeting the manager in person

The complaint will be recorded and investigated as quickly as is practicable and hopefully resolved.

If the complainant does not feel satisfied the manager will advise them to contact the Board of Families Fighting for Justice who will look at the available evidence and/or investigate further themselves and respond within one month with their findings.

Grievance Policy

- 1) The majority of problems encountered at work are usually capable of being resolved informally by the employee and the line manager concerned and thereafter the centre manager. There is however, a formal procedure which can be followed if a grievance cannot be resolved in this way. Details of the procedure are set out as below.
- 2) The object of the grievance procedure is to enable employees who consider they have a grievance or complaint arising from their employment with Families Fighting For Justice, to have it dealt with at the nearest appropriate level within as short a time as possible. Anyone wishing to use this procedure can do so freely and without prejudice to his/her position in the centre. Employees should not hesitate to use this procedure which has been adopted in recognition of the fact that whilst the Centre's policies are designed to encourage good working relationships, from time to time there may be circumstances, due to pressure of work or otherwise, in which

misunderstandings or grievances may arise. It applies to all employees, irrespective of job or grade.

- 3) Any grievance must be discussed initially with the immediate line manager and thereafter the centre manager who will attempt to resolve the matter after making such consultations as are necessary. You may be required to put any such grievance in writing. Every opportunity will be given for your grievance to be stated and thoroughly discussed. As appropriate, further investigation may take place and action taken.
- 4) At each stage of the procedure, you may choose to be accompanied by a fellow employee or trade union official to help put the case.
- 5) If the complaint or grievance relates to the centre manager or the matter is not resolved to your satisfaction within a reasonable time, the grievance can be raised in writing with the board. Having enquired into your grievance a member of the board (The investigating officer) will convene a formal hearing before two other members of the board (The hearing panel) to discuss the matter. You will be given at least 3 working days' notice of the grievance hearing. The investigating officer will state the findings of his/her investigation and you will be given an opportunity to thoroughly state your case. As appropriate, further investigation may take place and action taken.
- 6) The decision of the hearing panel will be notified to you in writing within 7 working days unless extended by mutual consent.
- 7) The decision of the hearing panel is final and the grievance procedure is exhausted following this stage.
- 8) All meetings will be private and confidential.

Families Fighting for Justice – Safe from harm policy

Families fighting for justice in accordance with its mission statement aims to help any individual regardless of background. Those individuals who have been in trouble with the police and may have a criminal record will not be discriminated against. However because of the nature of Families fighting for Justice and its activities, there are certain criminal offences we are not qualified or skilled to deal with. If, however the individual seeks help, we would refer them to other agencies more able and skilled than ourselves to deal with their particular needs.

The offences we cannot deal with are:

- Those convicted of sexual abuse, especially against children
- Those convicted of rape
- Those convicted of serious violent crime against another person

In the interests of safety for all concerned, as part of the conditions of acceptance on one of our courses the following disclosure must be completed. It must be stressed that this is in no way discriminatory, but merely a means of helping us to help you. All disclosures are treated in the strictest of confidence.

Families fighting for Justice – Child Protection Policy

Definition of Abuse

A child may be abused or neglected by inflicting harm or by failing to act or prevent harm. Children may be abused in a family or in an institutional or community setting by those known to them, or more rarely, by a stranger.

A duty to investigate

It is important that children (the Children Act 1989 defines a child as a person under the age of 18) are protected from abuse. The abuse may be of a physical, sexual or emotional nature. All complaints, allegations or suspicions must be taken seriously.

The centre is committed to working together with the local area Child Protection Committees (ACPC) and to complying with their procedures. It recognises that it has a responsibility towards young people within Families Fighting for Justice to safeguard and promote their welfare and to take appropriate decisions about how this can be achieved. It is not the centre's responsibility to investigate abuse. Nevertheless, it has a duty to act if there is a cause for concern and to notify the appropriate agencies so that they can investigate and take any necessary action.

The social services/police have the primary responsibility in the field of child protection. The Children Act 1989 places a duty on local authorities to take steps to protect children in appropriate circumstances and give certain powers to the police so that they can take action to protect children.

The Children Act 1989 defines a child as a person under the age of 18 years. "Working Together Under The Children Act 1989", published by the Department of Health sets out the governments guidance on child protection and says that all staff should be aware of the need to alert Social Services, the NSPCC or the police, when they believe a child has been abused or is at risk of abuse.

What is Child Abuse?

It can involve any one or more of the following:

- Neglect
- Physical injury
- Sexual Abuse
- Emotional Abuse

Procedure

This procedure must be followed whenever an allegation is made that a child has been abused or when there is suspicion that a child has been abused.

Promises of confidentiality should never be given to a young person as the matter may develop in such a way that these cannot be honoured.

If the complainant is the young person questions should be kept to the minimum necessary to understand what is being alleged and leading questions should be avoided. The use of leading questions can cause problems for the subsequent investigation and any court proceeding.

A full record shall be made as soon as possible of the nature of the allegation and any other relevant information including:-

- The date and time
- The place where the alleged abuse happened
- Your name and names of others present
- The name of the complainant and, where difference, the name of the child who has allegedly been abused.
- The nature of the alleged abuse.
- A description of any injuries observed.
- The account which has been given of the allegation.

Any person who has a suspicion that a child is believed to be suffering harm or is at risk of abuse should discuss the concern with the centre manager immediately.

Any suspicion, allegation or incident of abuse must be reported to the centre manager as soon as possible any in any even within 2 hours. A response should be given to the young person within 2 hours as to how the matter will be handled.

The nominate member of staff must report the matter to the local Social Services department, whether or not she/he feels that this action is justified in the particular circumstances of the case.

Some children with special educational needs (SEN) may need different treatment to other children e.g. in the way their physical/mental condition might mask possible abuse. Particular attention should be given to children with speech impediments as these can make communication difficult.

Families Fighting for Justice has a duty to make enquiries about the welfare of a child in their area if there is reasonable cause to suspect that the child is suffering or likely to suffer significant harm.

Procedures for all professionals and members of the public

If any employee or member of the public has reason to believe that a child may have been abused should always try to ensure that the child is safe. This should be the first priority and should surpass notification to the centre manager, social services or the police.

All instances or suspected instances of abuse of a child or young person must be discussed at once with your line manager and/or the manager of Families Fighting for Justice (Jean Taylor). **YOU ARE STRONGLY ADVISED FOR YOUR OWN BENEFIT AND FOR THAT OF THE CHILD/CHILDREN CONCERNED THAT YOU DO NOT DISCUSS THE INCIDENT WITH ANYONE OTHER THAN THOSE MENTIONED ABOVE.**

The person making the report should provide, where possible the child's name, date of birth and address with correct spelling. Any other information about the child/family would be helpful. Explain

clearly the nature of your concern. Ensure that social services know where the child is currently placed and give a contact number.

Families Fighting for Justice and O.L.L.Y

Safeguarding Whistleblowing Policy

**Review date
March 2024**

Whistle blowing policy to Safeguard and promote the welfare of children

Introduction

Improving the way in which people and organisations safeguard and promote the welfare of children is crucial to improving outcomes for children and young people and key local organisation named under section 11 of the Children Act 2004, have a duty to demonstrate that they have effective arrangements in place within their organisation to safeguard and promote the welfare of children. Keeping Children Safe in Education (2018) makes clear what arrangements must be in place within an organisation to safeguard and promote the welfare of children The Governing Body must demonstrate that it has an effective whistle blowing process in place and that the volunteers and students are aware of this process.

Policy Statement

Families Fighting for Justice and OLLY expects all volunteers, student including adults working with children and young people, contractors, or external agencies to express any concerns that they may have with regards to the conduct of any individual(s).

Families Fighting for Justice and OLLY is committed to the highest standards of openness, integrity, and accountability. All persons within this organisation must feel safe and supported to express their concerns.

This policy document is intended to encourage and enable our volunteers and students to raise their concerns and to do so without fear of victimisation or discrimination. It does not replace the Complaints Procedure or the Safeguarding including Child Protection Policy or the organisation's standard procedures for reporting allegations of concerns about volunteers or students. It is supplementary to the organisations Whistle Blowing Policy regarding other forms of malpractice covered under the 'Public Interest Disclosure Act'.

The Public Interest Disclosure Act (PIDA) protect the public interest by providing a remedy for individuals who suffer workplace reprisal for raising a genuine concern, whether it is a concern about child safeguarding and welfare systems, financial malpractice, danger, illegality, or other wrongdoing. The concern may relate to something that is happening or has happened in the past.

Aims

This policy aims to:

- Encourage adults working within the organisation to feel confident in raising concerns;
- Provide a process by which concerns can be raised and dealt with;
- Receive feedback on the process (where appropriate); and

- Provide a means by which the volunteers and students can receive support where concerns have been raised.

What does the safeguarding whistle blowing policy cover?

This policy is designed to cover concerns that volunteers and students have about the conduct of individuals in a position of trust within the organisation which could be detrimental to the safety or wellbeing of a young people and what volunteers or students, for whatever reason, **feel unable** to raise them under the organisations standard child protection procedures around dealing with such allegations. It would include issues about.

- Unprofessional behaviour
- Bullying by other students or volunteers
- Any form of abuse (physical, sexual, emotional or neglect)
- Name Calling
- Personal contact with children and young people which is contrary to the organisations policies and codes of conduct.
- Any form of racial abuse
- Inappropriate sexualised behaviour
- Knowledge about an individual's personal circumstances which may indicate that they could be a risk to children or unsuitable to work with children.

Please be mindful that these are examples of concerns and are not exhaustive.

Safeguarding against harassment or victimisation

Families Fighting for Justice and O.L.L.Y is committed to professional standards and to supporting its students and volunteers. It is recognised that the decision to report a concern is a difficult one to make. Harassment or victimisation will not be tolerated and Families Fighting for Justice and O.L.L.Y will take appropriate action to protect the person raising the concern when they are acting in good faith.

Confidentiality

All concerns will be treated in confidence, however, there may be a need for the whistle blower to give evidence for example if they have witnessed a crime or regarding disciplinary procedures if this is the outcome.

False Allegations

If a volunteer or student raises a concern in good faith, which is not confirmed by an investigation, no action will be taken. However, if a concern is raised maliciously, disciplinary action may be taken.

How to raise a concern

You should voice your concerns, suspicions, or uneasiness as soon as possible to the Lead Session Worker or Jean Taylor Founder

If you have any concerns about whistle blowing you can contact the Ofsted Whistle blowing hotline on 0300 123 3155 or alternatively email your concerns to [**whistleblowing@liverpool.gov.uk**](mailto:whistleblowing@liverpool.gov.uk)

**FAMILIES FIGHTING
FOR
JUSTICE**

**HEALTH & SAFETY
POLICY**

2023 - 2024

**THIS POLICY EXPIRES MAY
2024**

CONTENTS OF HEALTH & SAFETY POLICY

Sections

- 1. Health & Safety Management Team.**
- 2. Purpose Statement.**
- 3. General Policy.**
- 4. Statement.**
- 5. Company Policy for Health & Safety at Work.**
- 6. Company Induction Briefing.**
- 7. Procedures, Duties & Responsibilities.**
- 8. The Management of Health & Safety at Work Regulations 1999.**
- 9. General and Risk Assessment.**
- 10. The Workplace (Health, Safety & Welfare) Regulations 1992.**
- 11. The Health & Safety (Display Screen Equipment) Regulations 1992.**
- 12. The Control of Substances Hazardous to Health Regulations (COSHH) 2002.**
- 13. The Personal Protections Regulations 1992 (PPE).**
- 14. The Regulatory (Fire Safety) Reform Order 2005**
- 15. The Health & Safety First Aid Regulations 1981**
- 16. The Reporting of Injuries, Diseases & Dangerous Occurrences Regulations (RIDDOR) 1995.**
- 17. The Electricity at Work Regulations 1989.**
- 18. The Electricity Equipment (Safety) Regulations 1994.**
- 19. The Gas Safety (Management) Regulations 1996.**
- 20. The Noise at Work Regulations 2005.**
- 21. The Manual Handling Operations Regulations 1992.**
- 22. The Provision & Use of Work Equipment Regulations 1998.**
- 23. The Control of Asbestos At Work Regulations 2006.**
- 24. The Control of Work Related Road Safety.**
- 25. The Control of Work Related Solvents.**
- 26. The Food Safety Regulations 1995.**

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

Purpose Statement

Section 2 (3) of the Health & Safety at Work Act 1974 states:

It shall be the duty of every employer to prepare as often as may be appropriate to revise a written statement of his general policy. This will be with respect to the Health and Safety at Work of his employees and the organisation and arrangements for the time being in force for carrying out that policy, and to bring the statement, and any revision of it to the notice of all his employees.

Families Fighting For Justice

General Policy

It is the intent that FAMILIES FIGHTING FOR JUSTICE seek to provide the safest and healthiest-working conditions possible to all its employees waged, full time, part time, volunteers, trainees and service users. This is to also include any contractors or persons with specific business or permission at the premises of FAMILIES FIGHTING FOR JUSTICE .

FIGHTING FOR JUSTICE wish to stress the importance of the reading and compliance of Health & Safety documentation, and of good communications at all levels, at all times. The Senior Management Team and Health & Safety Advisor will regard failure in co-operations by any such persons as serious misbehaviour, leading to avoidable damage or accident. This will be treated as gross misconduct.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

STATEMENT

HEALTH AND SAFETY POLICY

Statement

FAMILIES FIGHTING FOR JUSTICE recognises and accepts the responsibility to provide safe working conditions, and believe that promotion of Health and Safety measures is a mutual objective for management, employees, volunteers, trainees and visitors.

To that end, FAMILIES FIGHTING FOR JUSTICE will take steps, so far as reasonably practicable, to provide:

- A safe place to work, with safe access and egress.
- A Healthy working environment.
- Sufficient information, instruction, training and supervision to enable all employees to avoid hazards and contribute positively to their own and others Health and Safety at work.

Whilst the company accepts that the general legal responsibility for the Health and Safety rests with them. It is also recognised that it is everyone's legal duty as laid down by section 7, of the Health & Safety at Work Act 1974, to take care of their own and other peoples Safety, and to co-operate with the organisation and its Advisors to enable it to carry out its responsibilities.

In particular staff have a duty to:

- Work safely, efficiently and without endangering the Health and Safety of themselves, their colleagues, the general public or any other person whom has a right of access to the organisations premises at any time.
- Adhere to Safety procedures laid down by FAMILIES FIGHTING FOR JUSTICE and to conform to all the instructions given by those with the responsibility for Health & Safety.
- Report all accidents at work, including injuries however slight to their Manager who will then inform the Health and Safety Advisor. It is the duty of the injured person to arrange for the details to be entered into the 'Accident Book'. It is the duty of the Site Managers to ensure that this is adhered to. Similarly, dangerous occurrences or accidents not resulting in injury should **always** are reported so that a reoccurrence may be prevented.

FAMILIES FIGHTING FOR JUSTICE, will under no circumstance tolerate any act of intimidation, intimidating situations, threats, potential violence or acts of violence to any member of staff

The Health and Safety Advisor will ensure that the accident reports meet statutory Safety obligations including that laid down in section 8 of the Act. This state's 'no person shall intentionally or recklessly interfere with or misuse anything provided in the interest of Health, Safety and welfare in pursuance of any relevant statutory provisions.'

All staff will be inducted into Health & Safety policy and made aware of their own responsibility as regards Health & Safety. It is the duty of the Site Manager to ensure each new staff member or volunteer is familiar with the Safety aspect of his or her job. A copy of this statement will be issued to The Chief Executive of FAMILIES FIGHTING FOR JUSTICE and copies will be readily available from him.

FAMILIES FIGHTING FOR JUSTICE will source information from the following authoritative bodies, professional Institutes and recognised organisations:

- HSE
- Environmental Health
- The Fire Officer
- Local Authority
- British Safety Council
- Institute of Occupational Safety & Health
- Chartered Institute of Environmental Health & Safety

The Organisations Health & Safety Advisor will review, update and constantly develop this working policy.

Signed.....

Mrs Jean Taylor

Date: 31st July 2019

Review Date: 31st July 2020

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

COMPANY POLICY FOR HEALTH & SAFETY AT WORK

Company Policy for Health & Safety at Work

1. General

The Health, Safety and welfare of employees, trainees, volunteers and visitors, is of prime importance to the company and is essential to the efficient operation of its undertaking. The responsibility for the Safety at work rests upon the Chief Executive. The Chief Executive will ensure that the policy is pursued throughout the company. The company will take all reasonable practicable precautions to ensure the Health, Safety and Welfare at Work of its employees, volunteers and visitors by providing:

- a) A safe working environment by the design, construction, operation and maintenance of all plant equipment and facilities.
- b) Safe systems of work.
- c) Adequate instruction, information, training and supervision.
- d) Control of all situations likely to cause damage to property and equipment.
- e) Effective facilities for the treatment of injuries that occur at work.
- f) Effective fire prevention and fire control procedure.
- g) Adequate facilities for consultation between the Chief Executive of FAMILIES FIGHTING FOR JUSTICE and its employees.
- h) The making of such tests, examinations, samples and records as are necessary to monitor the working environment. The results will be made known to The Chief Executive.

The company expects employees, volunteers and visitors to conform to this working policy and to comply with the relevant sections of the Health & Safety at Work etc. Act 1974, and to exercise reasonable care for their own Health & Safety and that of others who may be affected by their acts or omissions.

The overall responsibility for Health, Safety and Welfare of the company and its personnel is vested in the Chief Executive

The Chief Executive will give full backing to the Health and Safety Advisor of, whose function it shall be to monitor and operate the policy, and will support all those who endeavour to carry it out.

FAMILIES FIGHTING FOR JUSTICE reserve the right to review and update their policy periodically and as required by changes in legislation and applicable Regulations.

The Health & Safety Advisor will assist the Chief Executive by monitoring and reviewing the policy annually and periodically as updating and amendments are performed.

THE HEALTH & SAFETY AT WORK ETC ACT
1974

EMPLOYEES RESPONSIBILITIES

Employees have a duty to co-operate with their employer insofar as that employees must declare any information that will assist the employer to perform their business in a safe and healthy manner.

It is therefore reasonable for the employer to insist that the employee make known any condition whether medical or otherwise that may adversely affect the performance of the employee or that of others.

General duties of employees (s.7)

Two main duties are placed on an employee.

Section 7 (1)

To take reasonable care for the health & safety of them and that of others who may be affected by his acts or omissions at work.

Section 7 (2)

As regards any duty or requirement imposed on his employer or other person by or under any of the relevant statutory provisions, to co-operate with him insofar as is necessary to enable that duty or requirement to be performed by Families Fighting For Justice.

THE MANAGEMENT OF HEALTH & SAFETY AT WORK REGULATIONS 1999

Employees' duties (Regulation 14)

Every employee shall inform his employer (or the person responsible for health & safety matters):

(a). Of any work situation which a person with his training and instruction would reasonably consider to represent a serious and immediate danger to health & safety.

(b). Of any matter which a person with his training and instruction would reasonably consider represented a shortcoming in the employers protection arrangement for health & safety.

(This duty arises insofar as the situation affects the employee's own health & safety, or arises out of his own activities at work).

The ACOP points out those employees have certain duties under s.7 of the HSWA, but this Regulation goes much further. The employee must report to his employer any work situation, which might give rise to a serious or imminent danger to himself or to others if it flows from the work activity. Further he should report shortcomings in the employer's arrangements even when no danger exists so that the employer can take remedial action.

Date 31st July 2019

Review Date 31st July 2020

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

COMPANY INDUCTION BRIEFING

Health, Safety and Welfare Induction

Nature of Company

All persons will be briefed on the nature of the Company and the reasons to their specific task.

Company Site Location and Boundary

All persons will be made familiar with their surroundings with reference being made to existing and proposed work to be carried out by FAMILIES FIGHTING FOR JUSTICE. The persons will be briefed as they are instructed in their specific task.

Working Hours

The company work hours are contained in the Contract of Employment.

Specific Working Areas and Clients Restrictions

All persons will be informed of restricted areas. This restriction must be adhered to (except in cases of emergency). If for any unforeseeable reason they require access, they will report to their Manager requesting permission.

Fire Prevention Regulations and Emergency Procedures

All persons will be briefed on the following areas

- Smoking
- Electricity
- Position of fire extinguishers, and fire call points.
- Fire escape procedure
- Fire escape route
- Location of the hose
- Nearest telephone point
- Accident procedures
- First Aid Boxes
- Name of First Aider and Appointed Person

In respect to working at various locations. It is the duty of the Manager or his delegated person to ensure that fire precautions are within current workplace regulations at those particular premises.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

PROCEDURES, DUTIES AND RESPONSIBILITIES

NOTICE OF AGREEMENT

Procedures/ Duties and Responsibilities

The overall responsibility for the policy rests with the Chief Executive.

The Chief Executive will delegate some responsibilities for Health and Safety matters within the company.

The Chief Executive will be responsible for meeting any legal requirements in relation to the premises e.g. Fire Regulations and First Aid. It is recognised that in some instances Health and Safety matters will be dealt with immediately in view of risks.

The Health and Safety Manager will have the responsibility for the implementation of the policy.

The Chief Executive shall ensure co-operation and that all staff, volunteers, trainees and visitors comply with Health and Safety procedures in this policy. This includes the fabric of the building, heating, lighting and ventilation, security of the premises, electrical Safety, fire Safety and all other matters referred to.

Safety of Premises

Electricity and Lighting

The Chief Executive will ensure that lighting of offices, corridors, meeting rooms and stairways are adequate and suitable at all times when the building is in use.

Ventilation and Dust Control

The Chief Executive will ensure that adequate and suitable dust control and ventilation be used with particular emphasis in areas where equipment and appliances are used.

Maintenance

The Chief Executive will ensure that all equipment and appliances supplied by FAMILIES FIGHTING FOR JUSTICE and used by staff, trainees, volunteers and visitors is correctly used and regularly maintained.

The Chief Executive further accepts that all new and replacement equipment, appliances and substances incorporate the best practices on Safety and conform to all BS standards applicable.

Storage

The Chief Executive of FAMILIES FIGHTING FOR JUSTICE will ensure that all traffic routes and work permit areas are not cluttered with rubbish and such like. A safe means of storing materials and equipment will be provided. Staff or equipment will overcrowd no such office.

Guarding Excavations, Trap-ends and Openings

The Chief Executive will enforce Safety markings, barriers and guard-rails. They are to bring to the immediate attention any danger that could cause concern to the Health & Safety of any person on the premises. The above will conform to the current workplace (Health & Safety) Regulations 1992 Regulation 12 and 13. The barriers will be moved for supervised access purposes only. The above Regulations refer to the inside and outside boundaries of the premises, including the car park.

Body Protection

It is the intention of the Chief Executive to ensure that all persons are suitably dressed and fully protected for the task they are to perform. The current legislation is within the Health and Safety policy under the section Personal Protection Equipment Regulations 2002 (PPE).

Note: All Health and Safety legislation will be referred to during the Company Induction Programme.

NOTICE OF AGREEMENT

- a) A copy of this file is to be kept at each of the FAMILIES FIGHTING FOR JUSTICE administration offices at all times. A further copy of this document has been passed to the Chief Executive (Main Administration Base).
- b) This document is subject to updating as necessary and a formal annual review.
- c) All staff will read this document and persons authorised at the said Company, initially during induction, and then periodically as updating takes place.
- d) On induction each person will sign a certificate of compliance to the following:
 - I have read and fully understood the Health and Safety Policy Document of The Families Fighting For Justice
 - I agree to abide by their working health & safety policies and procedures

Signed.....

Name.....

Date.....

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

**THE MANAGEMENT OF HEALTH & SAFETY AT WORK
REGULATIONS 1999**

THE MANAGEMENT OF HEALTH & SAFETY AT WORK REGULATIONS 1999

The Health & Safety (Young Persons) Regulations 1997 As amended 1999

FAMILIES FIGHTING FOR JUSTICE recognises the above regulation, with regard to;

- Particular risks to young persons
- What we need to do to comply with the Regulation
- Specific restrictions on the work of young persons
- Compliance to the provision and use of work equipment regulations 1998 to young persons

Risk Assessment, Regulation 3

Regulation 3 requires a sufficient risk assessment of the Health and Safety risks to employees and others, to be undertaken with the appropriate control measures to be put into place. Included in the regulation, **is Any Act of Violence at Work that causes injury to any employee**, which is reportable under the RIDDOR regulations 2013

Risk Assessment Recording, Regulation 4

See Risk Assessment sheet within the Health and Safety Policy.

Risk Assessment Appropriate Action, Regulation 5

The Chief Executive will be advised by the Health & Safety Advisor of the appropriate action to be taken from the information given by Regulation 3.

In adherence to the above Regulations FAMILIES FIGHTING FOR JUSTICE recognise their duty to the Young Person Regulations that are incorporated into the Management of Health & Safety Regulations 1999.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

GENERAL RISK ASSESSMENT

RISK ASSESSMENT PROCEDURES

Who assesses risk?

FAMILIES FIGHTING FOR JUSTICE recognise their duty to assess hazards and risks to their employees and that of others. Site Managers and/or the Organisations Health & Safety Manager will perform and record such assessments.

What Risks will be assessed?

FAMILIES FIGHTING FOR JUSTICE will assess all hazards that have a potential to cause harm. All Site Managers have access to a competent Health & Safety Manager.

How thorough will the assessment be?

The Health & Safety Manager with competent and professional advice will assist the Site Managers.

When will assessments be performed?

Assessments will be performed prior to any change in operation, environment, individual or equipment. In general any type of change will require a new or revised assessment.

Will all assessments be recorded?

Yes all assessments are recorded and held in the appropriate document.

Reviewing the assessments

All assessments are reviewed annually and updated as required. Assessments are also monitored during Health & Safety performance audits.

What guidance is used during assessments?

The approved HSE guide 'Five Steps to Risk Assessment'
HSE 'A guide to Risk Assessments' INDG218

**FAMILIES FIGHTING FOR JUSTICE
GENERAL RISK ASSESSMENT**

Date.....

Hazardous Activity

Assessed Risk

Can Risk Be Eliminated **YES/NO** (delete)

Severity of Risk (Tick) High.....Medium.....Low.....

Likelihood of Occurrence High.....Medium.....Low.....

Risk High.....Medium.....Low.....

Where will risk occur?

When will risk occur?

Who will be affected?

Can risk be reduced? **YES/NO** (delete)

Method to Reduce Risk

.....
.....
.....
.....
.....
.....

Assessment of Risk

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

**THE WORKPLACE (HEALTH, SAFETY & WELFARE)
REGULATIONS 1992**

THE WORKPLACE (Health, Safety & Welfare) REGULATIONS 1992

Maintenance of Workplace, Equipment, Devices and Systems, Regulation 5

The Health & Safety Advisor will advise the Chief Executive with regard to the above regulation, to ensure its continuous and effective operation. The above will be identified by the Families Fighting for Justice - regulation 3 'Risk Assessment' of the Management of Health & Safety at Work Regulations 1992

Ventilation of the Workplace, Regulation 6

The Health & Safety Advisor will advise the Chief Executive with regard to the above regulation. The only exception being, where the use of breathing apparatus is necessary or specified. The Health & Safety Advisor will perform a risk assessment and meet periodically to discuss, check and record control methods applicable to regulation 6.

Temperature, Regulation 7

The Health & Safety Advisor will monitor temperatures during working hours by means of suitable thermometers in sufficient numbers.

Approved Code of Practice: 16 degrees Celsius and 13 degrees Celsius where physical effort is required.

Lighting, Regulation 8

Suitable and efficient natural light is achieved at FAMILIES FIGHTING FOR JUSTICE; however, due to atmospheric conditions artificial light source is readily available.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

**THE HEALTH & SAFETY (DISPLAY SCREEN
EQUIPMENT) REGULATIONS**

2007

THE HEALTH & SAFETY (Display Screen Equipment) REGULATIONS 2007

Definitions

- USE:** In connection with work
USER: An employee who habitually uses display screen equipment as a significant part of his/his normal work.

Regulation 2

FAMILIES FIGHTING FOR JUSTICE will perform a suitable and efficient analysis of the workstations, as used by the users and operatives. The findings will be used to assess the Health and Safety risks to which the operatives are exposed as a consequence.

Regulation 3

FAMILIES FIGHTING FOR JUSTICE will adhere to the above regulation, which requires them to ensure that all workstations must meet the requirements to the schedule of the regulations. To include workstation, ergonomics, work chair, light and heating.

Regulation 4

FAMILIES FIGHTING FOR JUSTICE will ensure that the work schedule is planned in order to allow periodic interruptions in order to eliminate RSI (Repetitive strain injury), eyesight defects, fatigue and stress.

Regulation 5

FAMILIES FIGHTING FOR JUSTICE will allow any user the opportunity to have an appropriate eye test after a request and at recommended regular intervals.

Regulation 6

FAMILIES FIGHTING FOR JUSTICE will endeavour to provide adequate Health and Safety training in the use of any workstation that an employee is required to work on. Furthermore, Training and Risk Assessments including control measures will be ongoing. Should the workstation be modified in anyway Regulation 7 will ensure that regulations 5 & 6 respectively are adhered too.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

**THE CONTROL OF SUBSTANCES HAZARDOUS TO
HEALTH REGULATIONS (COSHH)**

2002

THE CONTROL OF SUBSTANCES HAZARDOUS TO HEALTH REGULATIONS 2002 (COSHH)

FAMILIES FIGHTING FOR JUSTICE intends to prevent workplace disease with the use of a control framework

ASSESSMENT

CONTROL

MAINTENANCE

MONITORING

Regulation 6

FAMILIES FIGHTING FOR JUSTICE recognises that a suitable assessment is an essential requirement. The assessment will be a systematic review of the substance present, to include its form, quantity, effects, storage, handling, transportation, its affect and for how long.

Regulation 7

The use of Personal Protective Equipment (PPE) to be used, including (Regulation 8) FAMILIES FIGHTING FOR JUSTICE shall ensure that the PPE is properly used and those employees must make full and proper use of what is provided.

Regulation 9

FAMILIES FIGHTING FOR JUSTICE will maintain its control measures in working order and good repair.

Regulation 12

Suitable information and training will be given to an employee who undertakes work that may expose them to a substance that is hazardous to Health.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

THE PERSONAL PROTECTIVE EQUIPMENT REGULATIONS

1992

PERSONAL PROTECTIVE EQUIPMENT AT WORK REGULATIONS 1992 (PPE)

PLEASE NOTE THAT THE CHIEF EXECUTIVE REGARDS PPE AS A LAST RESORT. ALL EFFORT WILL BE MADE TO ENSURE THAT EVERY CONCEIVABLE CONTROL MEASURE IS EXHAUSTED.

Regulation 4

FAMILIES FIGHTING FOR JUSTICE will provide suitable PPE to each of its employees who may be exposed to any risk while at work, except where others have adequately controlled any such risk equally or by more effective means.

Regulation 6

The Manager, who will ensure it is used correctly, will supervise assessment of PPE.

Regulation 7

The Manager will ensure that all PPE is properly maintained and (Regulation 8) allow suitable accommodation for it to be stored correctly.

Regulation 9

FAMILIES FIGHTING FOR JUSTICE will ensure that adequate, appropriate, instruction and training will be readily available in the use of PPE.

Regulation 11

All employees must note that under the above regulation they are required to report any loss or defect of the equipment.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

THE REGULATORY (FIRE SAFETY)

REFORM ORDER 2005

Fire Reform Order 2005

The(Fire Safety) Reform order 2005

Fire precaution procedure will vary from location to location and task to task. If the Chief Executive is in doubt about fire precautions he will contact the Local Fire Advisor or the Health & Safety Advisor for advice.

General procedure in the event of fire.

If you discover a fire:

- Immediately operate the nearest alarm
- Call the fire brigade
- Leave the building and report the fire
- **DO NOT RE-ENTER THE BUILDING**

Fire Drills

These will be organised by the Operations Director.

It is the intent that the company ensures that no staff member, trainee, volunteer or visitor attempt to fight any fire unless previously trained.

Appropriate Fire-fighting equipment is installed (as advised) throughout the premises

Appropriate Emergency routes and exits are provided, and appropriately signed.

All equipment and devices provided are subject to a suitable system of maintenance.

Regulatory Reform (Fire Safety) Order 2005

The Regulatory Reform Order may only be used to reform existing legislation; it cannot be used to create an entirely new provision. A new burden may be imposed if it is linked to the removal of other onerous burdens.

FAMILIES FIGHTING FOR JUSTICE recognise their responsibilities in ensuring that:

The responsible person will make a suitable and sufficient assessment of the risks to which relevant persons are exposed. It will be performed for the purpose of identifying the general fire precautions they need to take, and to

comply with the requirements and prohibitions imposed on their Organisation under the order.

The responsible person will take such general fire precautions as will ensure so far as is reasonably practicable, the safety of any of his employees, and in relation to relevant persons who are not his employees. He will take such general fire precautions as may reasonably be required in the circumstances of the case to ensure that the premises are safe. The general fire precautions to be taken include:

- Measures to reduce the risk of fire on the premises and the risk of fire spreading.
- Measures in relation to means of escape
- Ensuring that the means of escape can be used effectively and safely
- Measures in relation to fighting fires on the premises
- Measures in relation to detecting fires on the premises
- Measures in relation to detecting fires and giving warnings
- Measures in relation to action to be taken in the event of fire, including instruction and training of employees and mitigation of the effects of fire

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

THE HEALTH & SAFETY (FIRST AID) REGULATIONS

1981

THE HEALTH & SAFETY (First Aid) REGULATIONS 1981

First Aid

The Chief Executive or his nominee is responsible for ensuring the provisions below are implemented. The nominated persons are:

Individual Site Managers

The Health & Safety Advisor

Training

FAMILIES FIGHTING FOR JUSTICE will use HSE approved organisations for its training.

First Aiders / Appointed Persons

These may be volunteers and no special liability is added by these Regulations. Should they be sued for any reason in connection with going to help someone in the workplace, Employers Liability Insurance will cover it.

First Aid Boxes

The appointed person will ensure that all First Aid boxes contain only approved items and nothing else, and ensure that monthly checks are made of the contents.

It is not part of the First Aiders responsibility or function to advise individuals to take drugs or to give them out. There will be no drugs of any description kept for these purposes.

Records / Notices

Within various locations of FAMILIES FIGHTING FOR Justice notice with the following information will be displayed:

Name of First Aider / Appointed Person

Location of:

Nearest Eye Injury Unit

Nearest Casualty Dept

Nearest Burns Unit

Nearest Coronary Care Unit

Accident at Work – Recording

The Site Manager will be responsible for reporting all accidents, which happen within the boundaries of their specific Site.

It is the injured person's responsibility to enter the details of the accident into the Accident Book. It is the Site Managers responsibility to ensure that it has been entered.

All persons are to be made aware of the importance of registering accidents.

Dealing with Accidents at Work

All persons will be briefed on induction in:

- Accident prevention
- Where the nearest First Aid boxes are kept
- Who is the First Aider or Appointed person

Prevention

Falling causes many accidents at work. Be aware of this, and report the following to the Estates Manager

- Spilt liquids
- Worn floor covering
- Slippery floor surfaces
- Trailing telephone or electric leads
- Missing or damaged handrails
- Fallen materials

The above list is not exhaustive.

Updating & review

The Health & Safety Advisor will annually update and review the list of Appointed Persons and First Aiders

In the event of an accident, it is the Site Managers responsibility to inform the Operations Director or his nominated person. The Operations Director or his nomination will inform the Health & Safety Advisor with immediate effect.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

**THE REPORTING OF INJURIES, DISEASES &
DANGEROUS OCCURANCES REGULATIONS (RIDDER)**

1995

THE REPORTING OF INJURIES, DISEASES & DANGEROUS OCCURRENCES REGULATIONS 1995 (RIDDOR)

The procedure for reporting deaths, major injuries and dangerous occurrences is set in detail in the company policy and associated documentation. A summary of the main requirements is set out below.

The following, must be reported immediately to the appropriate authority by the quickest practical method (usually by Telephone) and a report presented on the approved form within 10 days:

- Death of any person as a result of an accident at work.
- An accident to any person at work resulting in a major injury or serious condition specified in the Regulations.
- Any dangerous occurrences listed in the regulations (see summary below)

The H&S Manager will ensure:

- All fatal accidents must be reported to HM Coroner via the local Police Station.
The police have the right to investigate along with the Health & Safety Executive Inspectors.
- Form F2508 will be completed

Major injuries and serious conditions:

- Any fracture of any bones, other than to the fingers, thumbs or toes
- Any amputation
- Dislocation of the shoulder, hip, knee or spine
- Loss of sight (whether temporary or permanent) or any other listed eye injury
- Electric shock or burn causing unconsciousness, or requiring resuscitation, or hospitalisation for more than 24 hours
- Any injury leading to hypothermia, heat induced illness or to unconsciousness requiring resuscitation or admittance to hospital for more than 24 hours
- Acute illness or unconsciousness caused by any poisoning by any route
- Acute illness caused by exposure to material or biological agent.

Summary of reportable dangerous occurrences:

- Electrical short-circuit with fire or explosion
- Explosion or fire caused by any material resulting in any stoppage of work or plant for more than 24 hours
- Bursting, explosion or collapse, or fire involving a pipeline

Keeping records:

Records will be kept of all reportable deaths, injuries and dangerous occurrences. The particulars that will be kept are:

- Date and time of the accident or dangerous occurrences
- Injured person
- Full name and occupation
- Nature of injury

In the event of an accident to a non-employee

- Full name
- Status (e.g. Contractor, Staff, Customer, Visitor or Bystander)
- Nature of injury
- Place where accident or dangerous occurrences happened
- A brief description of the circumstances in which the accident or dangerous occurrences happened
- The date on which the event was reported to the enforcing authority
- The method by which the event was reported.

FAMILIES FIGHTING FOR JUSTICE would like it noted that the term “Accident” includes non-consensual physical violence done to a person at work.

Any assault on any employee is reportable under The RIDDOR 1995 Regulations, thus the Health and Safety Advisor will complete the appropriate form and forward it to the HSE who may fully investigate the matter. The Health and Safety Advisor will also complete an internal investigation.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

THE ELECTRICITY AT WORK REGULATIONS

1989

THE ELECTRICITY AT WORK REGULATIONS 1989

FAMILIES FIGHTING FOR JUSTICE shall ensure that all equipment purchased by themselves for use by their employees shall meet all applicable BS standards and carry a CE mark of conformity.

Risk assessments and evaluations, will be performed by the Health & Safety Advisor.

FAMILIES FIGHTING FOR JUSTICE will require all employees, to make full and proper use of any electrical equipment or system provided by them. All employees authorised to use the equipment will undergo tuition and training from the Chief Executive or appropriate supervisor.

FAMILIES FIGHTING FOR JUSTICE insist that **under no circumstances** may any employee waged or unwaged, volunteer, trainee or visitor, attempt to operate any electrical equipment or tamper with any electrical circuits, unless they have been trained or under supervision from a competent person. This duty is in addition to the general duties of employees under Regulations 7 & 8 of the Health & Safety at Work Act 1974.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

THE ELECTRICITY EQUIPMENT

(SAFETY) REGULATIONS

1994

THE ELECTRICITY EQUIPMENT (SAFETY) REGULATIONS 2016

FAMILIES FIGHTING FOR JUSTICE shall ensure that all equipment shall be:

- The **Electrical Equipment (Safety) Regulations 2016** implement the Directive into UK law. The **Regulations** apply to all **electrical equipment** that is designed or adapted for use between 50 and 1,000 volts (in the case of alternating current) and 75 and 1,500 volts (in the case of direct current) purchased after December 2016
- Safe
- Constructed in accordance with acceptable standards.
- Carry all applicable BS standards and a CE mark of conformity.
- Provide a level of protection to the user when connected to the electricity supply.

Risk assessments and evaluations, will be performed by the Health & Safety Advisor who may request assistance from a competent person.

FAMILIES FIGHTING FOR JUSTICE forbid any employee, visitor, volunteer, trainee or work placement to tamper or interfere with any electrical circuitry or equipment. The appropriately qualified and competent persons will receive authorised instruction from the Operations Director or Building Manager to perform such works.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

THE GAS SAFETY (MANAGEMENT)

REGULATIONS 1996

THE GAS SAFETY (MANAGEMENT) REGULATIONS 1996

Regulation 7 (1). Gas escape

FAMILIES FIGHTING FOR JUSTICE recognises that Transco has an absolute duty to provide a continuously staffed telephone service within Great Britain.

Regulation 7 (7). Responsible person

FAMILIES FIGHTING FOR JUSTICE shall ensure that if their responsible person for their premises knows of or has reason to suspect that gas is escaping from a gas fitting in those premises supplied with gas from a network, they shall immediately take all reasonable steps to cause the supply to be shut off at such a place as may be necessary to prevent further escape of gas.

Regulation 7 (8). Notify Transco

If gas continues to escape into the premises after the supply has been shut off or if the smell of gas persists, the responsible person carries the responsibility to immediately give notice to Transco.

Regulation 7 (9). Reconnection

Where an escape of gas has been stopped by shutting off the supply, no person shall cause or permit the supply to be re-opened, (other than in the cause of a repair by a competent person), until all necessary steps have been taken to prevent a recurrence of such escape.

In the event of an emergency evacuation.

No person shall re-enter a building following an evacuation that has resulted from a proven or suspected gas leak/escape. The following persons will authorise re-entry into the building:

1. A Transco Engineer
2. Fire Advisor or HSE Inspector (If in attendance)
3. An Operations Director
4. The Health & Safety Advisor

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

THE NOISE AT WORK REGULATIONS 2005

THE NOISE AT WORK REGULATIONS 2005

FAMILIES FIGHTING FOR JUSTICE will ensure that all reasonably practical methods will be used to ensure that noise is kept to a minimum both in the office and scheduled places of work.

Risk assessments will be carried out by the Site Manager or the Health & Safety Advisor.

FAMILIES FIGHTING FOR JUSTICE recognises that a competent person using the appropriately calibrated noise metering equipment must perform evaluations and monitoring.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

**THE MANUAL HANDLING OPERATION REGULATIONS
1992**

THE MANUAL HANDLING REGULATIONS 1992 amended in 2002

The Manual Handling Operations Regulations 1992, as amended in 2002 ('the Regulations') apply to a wide range of manual handling activities, including lifting, lowering, pushing, pulling or carrying.

The Regulations require employers to:

- avoid the need for hazardous manual handling, so far as is reasonably practicable;
 - assess the risk of injury from any hazardous manual handling that can't be avoided;
- and
- reduce the risk of injury from hazardous manual handling, so far as is reasonably practicable. This is a web-friendly version of leaflet INDG143(rev3), published 11/12 Health and Safety Executive Manual handling at work: A brief guide Page 2 of 10
- These points are explained in detail under 'Avoiding manual handling' and 'Assessing and reducing the risk of injury'

Employees have duties too.

They should:

- follow systems of work in place for their safety;
- use equipment provided for their safety properly;
- cooperate with their employer on health and safety matters;
- inform their employer if they identify hazardous handling activities;
- take care to make sure their activities do not put others at risk.

Avoiding manual handling Check whether you need to move it at all For example:

- Does a large work piece really need to be moved, or can the activity (eg wrapping or machining) be done safely where the item already is?

Controlling the risks

As part of managing the health and safety of your business, you must control the risks in your workplace. To do this you need to think about what might cause harm to people and decide whether you are doing enough to prevent harm. This process is known as a risk assessment and it is something you are required by law to carry out. A risk assessment is about identifying and taking sensible and proportionate measures to control the risks in your workplace, not about creating huge amounts of paperwork. You are probably already taking steps to protect your employees, but your risk assessment will help you decide whether you should be doing more. Think about how accidents and ill health could happen and concentrate on real risks – those that are most likely and which will cause the most harm.

The following might help:

- Think about your workplace activities, processes and the substances used that could injure your employees or harm their health. Health and Safety Executive Manual handling at work: A brief guide Page 3 of 10
- Ask your employees what they think the hazards are, as they may notice things that are not obvious to you and may have some good ideas on how to control the risks.
 - Check manufacturers' instructions or data sheets for chemicals and equipment, as they can be very helpful in spelling out the hazards.
- Some workers may have particular requirements, for example new and young workers, migrant workers, new or expectant mothers, people with disabilities, temporary workers.

Having identified the hazards, you then have to decide how likely it is that harm will occur. Risk is a part of everyday life and you are not expected to eliminate all risks. What you must do is make sure you know about the main risks and the things you need to do to manage them responsibly. Generally, you need to do everything reasonably practicable to protect people from harm. Make a record of your significant findings – the hazards, how people might be harmed by them and what you have in place to control the risks. Any record produced should be simple and focused on controls. If you have fewer than five employees you do not have to write anything down. But it is useful to do this so you can review it at a later date, for example if something changes. If you have five or more employees, you are required by law to write it down.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

**THE PROVISION & USE OF WORK EQUIPMENT
REGULATIONS 1998**

THE PROVISION & USE OF WORK EQUIPMENT REGULATIONS 1998

Regulation 4

FAMILIES FIGHTING FOR JUSTICE will ensure that work equipment supplied by them is suitable for the purpose for which it is used.

Regulation 5

FAMILIES FIGHTING FOR JUSTICE will ensure that the equipment is maintained, Further, (Regulation 7) users and supervisors will be given sufficient Health & Safety information and written instructions (if applicable) to the work equipment.

Regulation 11

FAMILIES FIGHTING FOR JUSTICE will take all reasonably practical measures to prevent access to dangerous parts of machinery; these measures will consist of guards and Safety devices as far as practicable.

Regulation 19

All work equipment supplied by FAMILIES FIGHTING FOR JUSTICE will have a means to isolate it from its means of energy. This will be visible, identifiable and accessible and all authorised users will be informed of the above.

Regulation 21

FAMILIES FIGHTING FOR JUSTICE will ensure that all places where work equipment is to be used will be suitably and sufficiently lit.

Regulation 24

All warnings will be appropriate for Health & Safety Regulations.

FAMILIIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

THE CONTROL OF ASBESTOS REGULATIONS 2012

THE CONTROL OF ASBESTOS REGULATIONS 2012

Control of Asbestos Regulations 2012

The Control of Asbestos Regulations 2012 (COAB) are designed to ensure the safe handling of asbestos, both for the benefit of those handling it, and the general public in the surrounding area.

Who has a duty to manage asbestos under COAB?

- Building owners
- Building managers, even if you have no formal contract to manage it
- If you are responsible for the building by way of a contract or tenancy agreement
- Those who have a duty to manage asbestos under COAB are called 'Duty Holders'.

What buildings are affected by COAB?

- Non-domestic buildings of any type
- Common areas of domestic buildings (e.g. stairwells, lift shafts, roof spaces)

All other domestic buildings are not affected.

What duties are imposed by COAB on Duty Holders?

1. You must find out if there is asbestos in the premises, its location and its condition. If a material may contain asbestos, you should assume that it does unless you have strong evidence to the contrary.
2. You must make and keep up to date a written record of the location and condition of any asbestos containing (or potential asbestos containing) materials in your property
3. You must assess the risk from any such material and plan how to manage that risk.
4. You must actively manage any risk caused by asbestos containing (or potential asbestos containing) materials.
5. You must provide this information to anyone who is working on and / or is likely to disturb that material.

How to identify asbestos

- Sprayed asbestos was used as fire protection in ducts and ceiling voids

- Lagging containing asbestos was used as thermal insulation for pipes and boilers
- Asbestos insulating boards were used as fire protection in wall partitions and ducts
- Asbestos cement products were used in water tanks and roofing
- Products containing asbestos were used in decorative plaster and paints
- Bitumen containing asbestos was used in roofing felt and ceiling tiles

If you suspect that asbestos is in your property, particularly if you plan to carry out renovation works, it is often best to instruct a specialist to carry out an asbestos survey. Organisations that sample and analyse asbestos are accredited by the United Kingdom Accreditation Service (UKAS). A list of UKAS accredited experts can be found at www.ukas.com/tools/contact-ukas.asp.

What to do if asbestos is discovered

If you discover asbestos in your premises, what action(s) you take will depend upon its condition.

Good condition:

- Monitor the condition of the material at regular intervals
- Where practical, label the material as containing asbestos
- Inform any contractor who is likely to work on or disturb the material about your concerns

Minor damage:

- Repair the material
- Monitor the condition of the material at regular intervals
- Inform any contractor who is likely to work on or disturb the material about your concerns

Poor condition:

- Any asbestos in poor condition should be removed by a suitably experienced and accredited contractor.

Likely to be disturbed:

- No matter what condition asbestos or asbestos containing products are in, if they are likely to be disturbed, they should be removed by an accredited contractor for safety reasons.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

THE CONTROL OF WORK RELATED ROAD SAFETY

2005

THE CONTROL OF WORK RELATED ROAD SAFETY 2005

HASAW Act 1974. (S2)

FAMILIES FIGHTING FOR JUSTICE recognises the Health & Safety At Work Act 1974 (S2), which requires them to ensure, so far as is reasonably practicable the Health and Safety of all employees while at work. This Act is intended to ensure that the public and other road users are not put at risk by work related driving activities.

Management of Health & Safety Regulations 1999. (S3)

Under the above Regulations FAMILIES FIGHTING FOR JUSTICE recognise their responsibility to ensure that work related driving risk assessments are performed by Site Managers (where Sites require employees to perform driving duties as part of their normal working duties).

Provision and Use of Work Equipment Regulations 1998 (PUWER)

FAMILIES FIGHTING FOR JUSTICE will ensure that any vehicle used for work purposes that is supplied by them will be suitable for its intended purpose, (Provision & Use of Work Equipment Regulations 1998)

(PUWER) Regulation 5

FAMILIES FIGHTING FOR JUSTICE will ensure that all of their company owned vehicles are maintained.

(PUWER) Regulation 7

Site Managers will ensure that users will be given sufficient Health & Safety information and written instructions (if applicable) to the familiarisation of the vehicle and its equipment.

Site Managers will evaluate the following risks:

The Driver – Competency

The Vehicle – Suitability *

The journey – Routes, scheduling, time, distance, weather conditions

Driving hours.

* Suitability of privately owned vehicles that are used for business use.

Do private vehicles carry the correct insurance and road licence?

Do private vehicles over 3 years old carry an appropriate MOT certificate?

It is the responsibility of Site Managers to ensure that staff who use their privately owned vehicles for company use, perform annual checks on the correct vehicle documentation. For example:

- The Correct insurance that covers business use
- A valid MOT Certificate (If applicable)
- A current road fund licence (Tax disc)
- A full driving licence

Site Managers must also ensure that company owned vehicles are not used for personal use without prior authorisation from their Site Manager. Staff will be made aware that personal use of company vehicles may lead to changes in a person's rate of tax.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

THE CONTROL OF WORK RELATED SOLVENTS

2005

THE CONTROL OF WORK RELATED SOLVENTS 2005

HASAW Act 1974 (S2)

FAMILIES FIGHTING FOR JUSTICE recognises the Health & Safety At Work Act 1974 (S2), which requires them to ensure, so far as is reasonably practicable the Health and Safety of all employees while at work. This Act is intended to ensure that employees, the public and others are not put at risk by work related use of solvents.

Management of Health & Safety Regulations 1999 (S3)

Under the above Regulations FAMILIES FIGHTING FOR JUSTICE recognise their responsibility to ensure that work related use of solvent risk assessments are performed by Site Managers (where Sites require employees to use such chemical substance as part of their normal working duties).

FAMILIES FIGHTING FOR JUSTICE will make known to all employees that different solvents may affect Health in a variety of ways. Short-term effects include:

Irritation, headache, nausea, dizziness and breathing problems.

FAMILIES FIGHTING FOR JUSTICE will make known to all employees how solvents can enter the body.

All employees will receive an initial induction and training prior to the use of solvents.

Comprehensive risk assessments will be performed.

Water and cleaning solutions will be readily available for all employees.

FAMILIES FIGHTING FOR JUSTICE will supply PPE and ensure that it is readily available for all employees. (PPE Regulations 1992).

FAMILIES FIGHTING FOR JUSTICE will ensure that the Workplace (Health & Safety) Regulations 1992 will be in force during any solvent operations.

FAMILIES FIGHTING FOR JUSTICE

HEALTH & SAFETY POLICY

THE FOOD SAFETY REGULATIONS

1995

(General Food Hygiene)

THE FOOD SAFETY REGULATIONS (General food hygiene) 1995

Management of Health & Safety Regulations 1999 (S3)

Under the above Regulations FAMILIES FIGHTING FOR JUSTICE recognise their responsibility to perform risk assessments relating to general food hygiene.

The Food Safety (General Food Hygiene) Regulations 1995

FAMILIES FIGHTING FOR JUSTICE will ensure that food –

- Preparation – Processing – Manufacturing – Packaging – Storing – Transportation – Distribution and Sale are carried out in a hygienic manner.

All employees will receive an initial induction and training prior to the preparation of food for human consumption.

A competent person will hold certified accreditation in the appropriate food preparation qualifications.

Water and cleaning solutions will be readily available for all employees.

FAMILIES FIGHTING FOR JUSTICE will supply PPE and ensure that it is readily available for all employees. (PPE Regulations 1992).

Food Safety (Temperature control) Regulations 1995

The temperature of food is controlled by the above Regulations.

FAMILIES FIGHTING FOR JUSTICE shall ensure that certain temperatures will be achieved and maintained during various related food processes and preparation.

Dermatitis

The Management of Health & Safety at Work Regulations 1999 and the Control of Substances Hazardous to Health 2005 require FAMILIES FIGHTING FOR JUSTICE to assess whether dermatitis is a risk. If an employee suspects that they are suffering from work related/occupational dermatitis, they must inform the Health & Safety Advisor who will request a doctor's confirmation. The Health & Safety Advisor must report any

confirmation to the HSE or the Environmental Agency under the RIDDOR Regulations 1995.

The most Senior Manager carries overall responsibility for the Health, Safety and welfare of:

- Employees
- Visitors
- Contractors
- Volunteers
- Members of the public.

Government authoritative bodies perform Fire, Environmental and Health & Safety enforcement for example:

HSE

Environmental Authority

The Local Fire Officer

Signed.....

JEAN TAYLOR

Date 31st July 2019

Review date 31st July 2020

OLLY Disciplinary Procedure

Disciplinary Rules

- OLLY requires good standards of discipline from its employees. These disciplinary procedures apply to any misconduct. The procedure is referred to in the Contract of Employment but is not contractual.
- The purpose of the procedure is to be corrective rather than punitive and it should be recognised that the existence of procedures such as these is to help and encourage the employee to achieve and maintain standards of conduct and attendance and to ensure consistent and fair treatment for all employees.
- If the employee conduct fails and, after warnings, remains below the level which is acceptable, they may be dismissed.
- The procedure will only apply to employees who have successfully completed their probationary procedure period. Probationary employees may be dismissed summarily for committing an act of misconduct during their probationary period. There will be no right of appeal against any such decision to dismiss in such circumstances.
- Summary dismissal without notice will take place if an act of gross misconduct is committed. Gross misconduct is any deliberate act by an employee that is detrimental to the good conduct of the charity's name. Examples of misconduct and gross misconduct are listed below.

Examples of gross misconduct

The following is a non-exhaustive list of examples of offences which amount to gross misconduct:

- Dishonesty
- Falsification of charity records
- Failure to comply with relevant statutory or regulatory requirements.
- Violent, abusive, or intimidating conduct
- Deliberate damage to charity's property
- Sexual, racial, or other harassment
- Unauthorised use or disclosure of confidential information
- Attending work under the influence of alcohol or non-medically prescribed drugs
- Rudeness to clients/beneficiaries
- Any action likely to bring the charity into disrepute.

- Accepting a gift which could be construed as a bribe.
- Sleeping on duty
- Breach of Health and Safety rules which endanger the health and safety of others.
- Failure to disclose correct information in the employee's application for employment
- Conviction for any serious criminal offence whilst an employee of OLLY

Disciplinary Hearings

- No disciplinary action will be taken until the case has been fully investigated.
- At all stages, the employee will be advised of the nature of the complaint and will be given the opportunity to state their case before a decision is made.
- The employee may, if they wish, be accompanied by a fellow employee or a trade union official of their choice at any disciplinary hearing.

Disciplinary Procedure

Except for acts of gross misconduct, the following procedure will normally be adopted:

- For minor breaches of discipline, or failure to achieve satisfactory standards, the line manager will give a formal verbal warning normally. This will lapse after 6 months in the absence of further offences.
- For more serious offences, or in the event of further minor transgressions, a warning will be given in writing. The line manager will normally give this warning. This lapse after 12 months in the absence of further offences.
- In the event of further repetition of the misconduct or a failure to comply with a requested improvement, or in the case of misconduct or failure to comply with standards which do not amount to gross misconduct, but which warrant a first and final warning, a final written warning will be issued by the line manager. This warning will specify that the consequences of a failure to comply will normally be dismissal. This will lapse after 12 months in the absence of further offences.
- In the event of any further misconduct or failure to achieve satisfactory standards or in the case of misconduct not amounting to gross misconduct but warranting dismissal, dismissal may result.
- In the cases of gross misconduct, the employee will normally be dismissed without notice or pay in lieu of notice or of accrued holiday pay. In exceptional circumstances, alternative disciplinary action may be taken.

Rules of suspension of staff

- Suspension will be on full pay and the employee will be informed in writing of this at the time.
- The suspension will not normally be for more than five days.

Appeals

- If the employee is dissatisfied with any disciplinary decision affecting them, they may appeal to OLLY Trustees (The management board) within five working days of the disciplinary decision.
- If the disciplinary action which is the subject of the appeal is the employee's dismissal the decision to dismiss will stand unless it is reversed on appeal.
- Any appeal must be put in writing, stating the grounds for the appeal. The appeal will be heard by two members of the Management Board (Appeal Panel) provided they have not been involved in the initial proceedings. The appeal will review but cannot increase a disciplinary penalty.
- The decision of the Appeal Panel is final. There is no further right of internal appeal.

Families Fighting for Justice and O.L.L.Y
(Our Lost Love Years)
Staff Supervision Policy/Procedure

Reviewed 1st March 2023

Aims and Objectives

To review an individual's performance and progress in a job

Staff supervision will improve the employee's performance, help in career planning, and assist the employee to evaluate their own performance to develop themselves.

Evaluation of Staff

Staff will be evaluated through the following methods:

- Trial period reports and probationary period; all new staff complete a six-month probationary period.
- Regular staff supervision: the aim is to review tasks and work set for employees and to mutually discuss the different aspects of work.
- Appraisal forms and meeting every 3-6 months.

Procedure

1. Trial period reports and supervision will be carried out with all employees.
2. Line manager will notify employees in advance of date and time of any of the above meetings to be held.
3. Relevant documents are completed during these meetings and are signed and dated by both line manager and employee. They will be kept in staff files.

4. Documents will be used to monitor and track employee's performance and training needs.

YOU DO NOT NEED TO WAIT FOR THESE OPPORTUNITIES TO DISCUSS ANY MATTERS WITH THEIR LINE MANAGER.

Families Fighting for Justice and OLLY (Our Lost Love Years)

PHOTOGRAPHY POLICY

Reviewed 1st March 2023

Children's and young people's names will not be used in photography captions.

Parental/carers permission will be obtained for a child to be photographed/videoed

When appropriate permission will be sought from the child/young person to use their image
Image

Images of children/young people will only be used are if they are in appropriate in suitable dress to reduce the risk of inappropriate use

No images used on OLLY'S/FFFJ website will include information about the child/young person, preventing an individual to learn more about them

Written expectations will be given to professional photographers or the press who are invited to an event, making clear the organisation's expectations of them in relation to child protection

Photographers will not have unsupervised access to children.

For school children who visit our centre for school programmes will be sent a letter requesting permission to take pictures and videos during the programme for our website. The school will then return any letters from parents that have requested for their child **NOT** to be videoed and or photographed

Families Fighting for Justice and O.L.L.Y

(Our Lost Love Years)

Working in Partnership with Parents and Carers

Policy Aim

O.L.L.Y and Families Fighting for Justice recognises that working in partnership with parents/carers is of major value and importance to the provision in enabling it to provide a happy, caring, and stable environment for children and their parents. The provision should aim to form a good relationship with parents/carers so that information regarding their children (be it development, social or health related) can be exchanged easily and comfortably by staff and parents.

The list below shows ways in which the provision should try to achieve a strong working partnership with parents/carers:

- A member of staff is always available for discussion with parents/carers. Arrangements can be made for more private discussions at agreed times;
-
- Information provided by parents/carers about their children will be kept confidential and treated on a strict need-to-know basis.
- Information regarding the children's activities throughout the day will be sent to the parents/carers prior to the children's visit.
- If the staff have any concerns about the child's well-being during the day every effort will be made to contact the parents or their emergency contact;
- Parents/carers are requested to keep us informed of any changes to personal circumstances, which may have an effect upon a child, e.g. change of address, telephone number, doctor, emergency contact. Parents/carers are also requested to keep us informed of any circumstances which could have an effect on a child's emotional wellbeing, e.g. bereavement, separation or illness in family.

Families Fighting for Justice and O.L.L.Y (Our Lost Love Years)

Smoke free Policy

1. Introduction

This smoke free policy has been adopted by Families Fighting for Justice and O.L.L.Y with the aim of:

1.1 Creating a smoke free early year setting, this includes all outreach venues where services are delivered that both children and parents attend, including client's homes when staff must visit. This promotes and supports smoke free lifestyles.

1.2 The objectives of the policy are to:

- ✚ protect all children, parents and career's, employees and visitors from exposure to secondhand smoke and vapour in our office/Centre
- ✚ support those volunteers, students and clients who are smokers and wish to stop smoking, and
- ✚ Proactively promote the smoke free agenda.

1.3 The policy provides guidance for volunteers and students and users of the setting on why we are a smoke free centre and what this means in practice. The policy applies to everyone using the premises (including all grounds and buildings) for any purpose, at any time.

E-cigarettes and Vaping;

Smoking is defined clinically and in law. E-cigarette use does not meet the definition in either context. E-cigarettes carry a fraction of the risk of cigarettes and have the potential to drive down smoking rates and improve public health.ⁱ

1.4 The use of e-cigarettes is covered under this policy. Although the evidence does not currently show e-cigarettes to be acting as a gateway into smoking for young peopleⁱ, there is still concern that allowing their use on-site could threaten what has become the norm of not smoking in our Office/Centre. Although E-cigarettes are around 95% safer than smokingⁱⁱ so can be a useful quitting aid for some individuals, vaping is discouraged within in early years settings and schools due to the role modelling from adults and mimicking behaviour of children.

1.5 People with asthma and other respiratory conditions can be sensitive to a range of environmental irritants, which could include e-cigarette vapour, therefore the use of e-cigarette around children is discouraged.

1.6 E-cigarette use is illegal for under 18's. In the UK protection is in place via prohibitions on the sale of e-cigarette to under 18's and purchase by adults on behalf of under-18sⁱⁱ.

2. Rationale

DIRECT QUOTE FROM TOBACCO CONTROL PLAN FOR ENGLAND (2017)

“The UK has made great strides in reducing the harms caused by smoking, but it still remains the leading cause of preventable illness and premature death in England. Smoking prevalence has substantially reduced; 20.2% of adults smoking at the start of the plan, (2011), to just 15.5% now. the lowest level since records began. But whilst we have made great strides in the right direction, there is more to doⁱⁱⁱ.”

- ✚ Every year, around **80,000 smokers in the UK die from smoking related causes: over 200 deaths every day.**
- ✚ Smoking accounts for over one-third of respiratory deaths, over one-quarter of cancer deaths, and about one-seventh of cardiovascular disease deaths.
- ✚ **About half of all regular cigarette smokers will die prematurely, losing on average around 10 years of life.**
- ✚ There are still about **6 million adults** who smoke cigarettes in Great Britain.
- ✚ **Nationally 8.2% of 15-year-olds still smoke. This figure is 10% in Devon, risking a lifetime of ill health.**
- ✚ **Smoking rates have remained stubbornly higher amongst those in our society who already suffer from poorer health and other disadvantages. Smoking rates are almost three times higher amongst the lowest earners, compared to the highest earners.**
- ✚ Smoking prevalence is **highest in the 25-34 age group (25%)** and lowest amongst those aged 60 and over.^v
- ✚ **Nationally 10.6% of pregnant women still smoke and in Devon this figure is 12.3%^{iv}.** Smoking in pregnancy can cause increased risk of miscarriage, stillbirth, preterm birth and low birth weight. It has been found to increase infant mortality by about 40%^{vi}.

3. National strategy and legislation

- 3.1 This policy is informed by Healthy Lives, Healthy People: A Tobacco Plan for England (2011). It supports compliance with Health & Safety Legislation and Employment Law. The Health Act 2006 bans smoking in all enclosed public spaces and section 2(2) of the Health and safety at Work Act 1974 places a duty on employers to:

'...provide and maintain a safe working environment which is, so far as is reasonably practical, safe, without risks to health and adequate as regards facilities and arrangements for their welfare at work.'

Families Fighting for Justice and O.L.L.Y
(Our Lost Love Years)

TIME KEEPING AND ATTENDANCE

Attendance and time keeping are viewed as a vitally important issue at OLLY/FFFJ since children's progress and achievement cannot be maximized unless children attend regularly and on time.

During our school programme children are expected to arrive with their class, only in exceptional circumstances will children be allowed in after this.

Children are expected to arrive by 9.30 if attending our out of school programme.

Children arriving after this will not be admitted unless contact has been made with the centre to explain the lateness.

As a member of team OLLY/FFFJ you are expected to arrive at your agreed time

Families Fighting for Justice and O.L.LY (Our Lost Love Years)

SPECIAL EDUCATIONAL NEEDS POLICY

Introduction

We at OLLY/FFFJ support children and young people in a manner that acknowledges their entitlement to share the same learning experiences that their peers enjoy. Wherever possible, we do not withdraw children and young people from the classroom situation. As we already practice, to maximise learning, we ask the children and young people to work in small groups.

Children and young people's education should promote their physical, mental, moral, cultural, spiritual, emotional, and social development. At OLLY/FFFJ we recognise that every child and young person has unique characteristics, interests, abilities and learning needs.

This centre provides a broad and balanced programme for all children. When planning, the education team are designated to set appropriate learning challenges and respond to children's diverse learning needs. Some children and young people have barriers to learning that means they have special needs and will require additional support by our education team. These requirements are likely to arise because of a child or young person having special educational needs. The education team take account of these requirements and make provisions where necessary, to support individuals or groups of children or young people, and thus enable them to participate effectively in all activities. Such children and young people may need additional or different help from that given to the other children or young people of the same age.

Aims and Objectives

- To create an environment that meets the special educational needs of each child and young person.
- To ensure that the special educational needs of children and young people are met.
- To make clear the expectations of all staff involved.
- To identify the roles and responsibilities of staff in providing children's and young people's special educational needs.
- To enable all children and young people to have full access to all elements of the centre programme.

Educational Inclusion

In our centre we aim to offer excellence and choice to all our children and young people, whatever their abilities or needs. We have high expectations of all our children and young people. We aim to achieve this through the removal of barriers to learning and participation. We want all our children and young people to feel that they are a valued part of our centre community. Through appropriate curricular provision, we respect the fact that children and young people:

- Have different educational needs and aspirations.
- Require different strategies for learning.
- Acquire, assimilate, and communicate information at different rates.
- Need a range of different teaching approaches and experiences.

Centre staff responds to children's and young people's needs by:

- Providing support for children who need help with communication, language, and literacy.
- Planning to develop children's understanding using all available senses and experiences.
- Planning for children's full participation in learning, and in physical and practical activities.
- Helping children to manage their behaviour and take part in learning effectively and safely.
- Helping individuals to manage their emotions particularly trauma or stress and to take part in learning.

What are Special Needs?

The law says that children and young people have special educational needs if, 'they have a learning difficulty, which calls for special educational provision to be made for them'. According to the Revised Code of Practice 2002, children and young people have special needs if they have 'significantly greater difficulty in learning than most children of the same age or have a disability which prevents or hinders them from making use of educational facilities of a kind generally provided for the children and young people of the same age.' The Disability Discrimination Act defines anyone with a disability as having, 'a physical or mental impairment which has a substantial and long term adverse effect on the ability to carry out normal day to day activities.'

Children's or young people's special needs may be places in one or more of the following categories:

- Learning.
- Communication and interaction.
- Physical, medical, and sensory.
- Social, emotional and/or behavioural.

Children and young people with special education needs have learning difficulties that call for special provision to be made. All children and young people have special needs at some time in their lives. Children and young people have a learning difficulty if:

- They have significantly greater difficulty in learning than the majority of children the same age.
- They have a disability which prevents or hinders them from making use of the educational facilities which are provided for children and young people of the same age.

In most cases children and young people join our centre with their needs already assessed. We then use this information to provide differentiated activities according to the child's abilities and needs.

Access to the learning programme

All children and young people have an entitlement to all aspects of the programme, which is differentiated to enable children to:

- Understand the relevance and purpose of activities.
- Experience levels of understanding and rates of progress that bring feeling of success and achievement.

The education team endeavour to provide resources and use a range of strategies to meet children's special educational needs. Lessons have clear learning objectives; we differentiate, work appropriately, and use informal assessments to inform the next stage of learning.

We at OLLY/FFFJ support children and young people in a manner that acknowledges their entitlement to share the same learning experiences that their peers enjoy. Wherever possible, we do not withdraw children from the classroom situation. As we already practice, to maximise learning, children work in small groups.

Children and young people's participation

In our centre, we encourage children and young people to take responsibility and to make decisions. This is part of the culture of our centre and relates to children and young people of all ages.

COMMUNICABLE DISEASE POLICY PROCEDURE

Reviewed 1st March 2023

OLLY COMMUNICABLE DISEASE POLICY/PROCEDURE

POLICY AIM

Any child will not be knowingly accepted into the centre if they are showing signs/symptoms, or the manager has reason to believe that the child may have any of the following: -

Chicken pox-fever, itchy rash, blister like appearance - To **prevent** spreading the infection, **keep children off** until all **their** spots have crusted over. **Chickenpox** is infectious from 1 to 2 days before the rash starts, until all the blisters have crusted over (usually 5 to 6 days after the start of the rash).

Vomiting and **diarrhoea**. - **Children** with these conditions **should** be kept **off**. They **can** return 48 hours after **their** symptoms disappear. Most cases of vomiting or **diarrhoea** get better without treatment, but if symptoms persist, consult your GP.

Fever (38 degrees c- 100 degrees f)

Gastroenteritis is a very common condition that causes diarrhoea and vomiting. It's usually caused by a bacterial or viral tummy bug.

It affects people of all ages, but is particularly common in young children.

Most cases in children are caused by a virus called rotavirus. Cases in adults are usually caused by norovirus (the "winter vomiting bug") or bacterial food poisoning.

Gastroenteritis can be very unpleasant, but it usually clears up by itself within a week. You can normally look after yourself or your child at home until you're feeling better.

German Measles- slight cold, sore throat, swollen glands, pink rash - Important. Stay **off** for 5 days after **the** rash appears. Also try **to** avoid close contact with pregnant women. **Rubella** is infectious from 1 week before **the** symptoms start and for 4 days after **the** rash first appears

Impetigo – The symptoms of non-bullous impetigo begin with the appearance of red sores – usually around the nose and mouth but other areas of the face and the limbs can also be affected.

The sores quickly burst leaving behind thick, golden crusts typically around 2cm across. The appearance of these crusts is sometimes likened to cornflakes stuck to the skin.

The symptoms of bullous impetigo begin with the appearance of fluid-filled blisters (bullae) which usually occur on the central part of the body between the waist and neck, or on the arms and legs. The blisters are usually about 1-2cm across.

The blisters may quickly spread, before bursting after several days to leave a yellow crust that usually heals without leaving any scarring.

Impetigo is a common and highly contagious skin infection that causes sores and blisters. It's not usually serious and often improves within a week of treatment or within a few weeks without treatment.

Measles-high fever, runny nose and eyes, a cough, white spots in mouth - **Measles** is most infectious from four days before **the** rash appears until four days afterwards. A **child should** be kept **off school** for four days after **the** onset of **the** rash.

Meningitis – fever, vomiting, headache, stiff neck, dislike of bright lights, rash, seizures - Most cases of viral **meningitis** end within **7 to 10** days. Some people might need **to** be treated in **the** hospital, although most teens **can** recover at home if they're not too ill.

Mumps – pain and swelling of jaw - People with **mumps should** therefore stay **off** and avoid other people as much as possible. This is as **soon** as **mumps** is suspected and for five days from **the** onset of parotid gland swelling.

Scabies – bumps on the skin usually filled with pus on the face neck palms and soles - **Scabies** mites generally do not survive more than 2 to 3 days **away** from human skin. **Children** and adults usually **can** return to **child** care, **school**, or work the day after treatment.

Scarlet fever – loss of appetite, pale around the mouth, bright pinpoint rash - If your **child** has **scarlet fever**, **keep** them **away** for at least 24 hours after starting treatment with antibiotics. Adults with **the** illness **should** also stay **off** work for at least 24 hours after starting treatment.

Whooping Cough – snuffly cold, cough and a whoop, vomiting - If you or your **child** are taking antibiotics for **whooping cough**, you need **to** be careful not **to** spread **the** infection **to** others. Stay **away** until 48 hours from **the** start of antibiotic treatment or three weeks after **the coughing** bouts started (whichever is sooner).

Any decision will be made with the child's welfare in mind

Please inform us as soon as possible if your child has any of the above. This will enable us to make other parents aware of the possible spread of infection

If your child has Sickness or Diarrhoea please make sure that your child is 48 hours clear after last incident before your child attends any Sessions

If you notice a case of Knits please inform a session Worker

COMMUNICABLE DISEASES PROCEDURE

In the case of a visiting school responsibility will be passed onto the teacher who is accompanying the child. OLLY staff will then document this.

In the case of activities organised and run solely by the charity ie. Easter or Summer clubs a member of the OLLY staff will contact the parent/carers. If this is unsuccessful we will then telephone the emergency contact number and inform them.

The child will be cared for in an appropriate way until they are collected, the child will not be left alone at any time

It is OLLY staff responsibility to keep the child until they are collected. Depending on the illness the child will be isolated and kept comfortable in the sickness area If symptoms worsen our staff will call an ambulance

A member of staff will accompany the child to hospital during our out of school themed weeks. During the schools programme it will be the responsibility of the visiting staff

Covid 19 Virus

Do not leave home if you or someone you live with has any of the following:

a high temperature

a new, continuous cough

a loss of, or change to, your sense of smell or taste

To protect others, you must stay at home if you or someone you live with has symptoms of coronavirus (COVID-19).

Information:

If you think you might have coronavirus, check if you need to self-isolate using the 111 online coronavirus service.

Can I leave my home if I am self-isolating?

If you or someone you live with has symptoms of coronavirus:

do not leave your home for any reason – if you need food or medicine, order it online or by phone, or ask someone to deliver it to your home

do not have visitors in your home – including friends and family

do any exercise at home – you can use your garden if you have one

How long to self-isolate

If you have symptoms

If you have symptoms of coronavirus, self-isolate for 7 days.

After 7 days:

you can stop self-isolating if your symptoms have gone, or if you just have a cough or changes to your sense of smell or taste – these symptoms can last for weeks after the infection has gone
keep self-isolating if you have any other symptoms (such as a high temperature, runny nose, feeling sick or diarrhoea) – you can stop self-isolating when your symptoms have gone

If you live with someone who has symptoms

If you live with someone who has symptoms, self-isolate for 14 days from the day their symptoms started.

This is because it can take 14 days for symptoms to appear.

If more than 1 person at home has symptoms, self-isolate for 14 days from the day the first person started having symptoms.

If you get symptoms while self-isolating – you should self-isolate for 7 days from when your symptoms started, even if it means you are self-isolating for longer than 14 days.

If you do not get symptoms while self-isolating – you can stop self-isolating after 14 days.

After self-isolation

When you stop self-isolating, it is important to follow the advice on social distancing.

This means you should stay at home as much as possible. But you can go out to work (if you cannot work from home) and for things like getting food or exercising.

If you are a health or care worker, check with your employer before going back to work.

If you have symptoms and live with someone at higher risk from coronavirus

If you live with someone who is 70 or over, has a long-term condition, is pregnant or has a weakened immune system, try to arrange for them to stay with friends or family for 14 days.

If you must stay at home together, try to keep 2 metres (3 steps) away from each other. If possible, try not to share a bed.

How to reduce the spread of infection in your home

Do

wash your hands with soap and water often, for at least 20 seconds

use hand sanitiser gel if soap and water are not available

cover your mouth and nose with a tissue or your sleeve (not your hands) when you cough or sneeze

put used tissues in the bin immediately and wash your hands afterwards

clean objects and surfaces you touch often (such as door handles, kettles, and phones) using your regular cleaning products.

clean a shared bathroom each time you use it, for example, by wiping the surfaces you have touched

Do not

do not share towels, including hand towels and tea towels.

O.L.L.Y (Our Lost Love Years)

EMERGENCY PROCEEDURE POLICY

In the event of an emergency arising such as a fire, gas leak, bomb scare or a critical incident outside the centre the following procedures must be followed:

If the fire alarm sounds all occupants of the building will be evacuate by the nearest available exit and go directed to the Assembly point located in the OLLY car park.

On an outing an Assembly point will be confirmed.

Visitors to the centre including adults and children will be made aware of our fire procedures during their induction.

The administration staff are responsible for telephoning the emergency services 999 and taking the registers, including visitors' book, to the Assembly point. Registers are taken at assembly point to ensure nobody is left in the building. Emergency services will be informed if there is anyone left inside the centre.

PROCEDURE TO BE FOLLOWED UPON HEARING THE FIRE ALARM

Staff should lead by example by staying calm at all times.

Stop whatever you are doing and instruct the children to do the same.

Leave all personal belongings behind

Close all the windows.

Gather the children at the fire exit.

Ensure all doors are closed behind you.

All children should be evacuated from the building as quickly and as calmly as possible.

Remember to stay calm and to keep the children calm.

Ensure that a member of staff checks all rooms.

DO NOT USE LIFT: In the eventuality of a child/adult who needs to use the lift, they would be carried down the stairs with assistance.

Administration staff will collect the registers, first aid kit and phone the fire brigade.

All children and staff will meet at the designated assembly point: The OLLY car park, outside Bensons for Beds back doors or outside on Riding Street (All children and visitors' will be informed of the assembly point during their induction)

The register is to be taken as soon as everyone who can get out has assembled at the assembly point. Fire fighters can now be informed of anyone still trapped inside the building.

No Children are to leave the assembly point without the consent of the person in charge (Lee McVoy) if unavailable a person will be designated.

Any child who is collected during an evacuation must be signed out by the parents/main carer on the register so there can be no confusion as to where the children are. Whilst outside children should be kept calm and in the designated area. Once the fire brigade has proclaimed the building safe staff and children can re-enter the building. Once inside the register will be retaken.

In the case of a gas leak a member of staff will turn the gas supply off if safe to do so. The gas main is situated in the staff kitchen underneath the sink. A member of staff will check all the rooms to make sure there is nobody left in the building. A member of the administration team will ring, British Gas on (0800-111-999) Follow the evacuation procedure.

In the case of a caller claiming there is a bomb or similar threat to the centre. Evacuate the building by raising the alarm and following the evacuation procedure. The emergency services will be alerted.

Families Fighting for Justice and O.L.L.Y

(Our Lost Love Years)

Drug and Alcohol Policy

POLICY AIM

OLLY is committed to providing a safe and productive work environment and to promote the health and safety, and well-being of all its employees. The drug and alcohol policy are designed to ensure that all employees are aware of the health risks associated with drug/alcohol misuse, outline the help and support available for these issues and set out the consequences for those who are found to be using drugs or alcohol at work.

The inappropriate use of alcohol and drugs can damage the health and well-being of employees and have reaching effects on their personal and working lives. At work alcohol and drug misuse can lead to reduced level of attendance, sub-standard work performance and increased health and safety risks.

OLLY/FFFJ treats drug and alcohol dependency as a health problem that requires special help rather than a disciplinary matter although OLLY reserves the right to take disciplinary action to deal with the problem if this is inappropriate.

This policy covers the misuse of intoxicating substances, which include alcohol, substances, legal and illegal drugs, prescription and over the counter medicines and other substances that could adversely affect work performance and/or health and safety.

This policy also positively discourages the drinking of alcohol during the working day and no alcohol is to be consumed 12 hours prior to the start of your working day.

This policy aims to:

- Raise staff awareness to the risks and the potential harm to health associated with the misuse of intoxicating substances.
- Set out the support available to employees who may be misusing drugs or alcohol and encourage them to seek help.
- Set out rules regarding the use of intoxicating substances in the workplace so that employees are aware of the likely consequences for their employment of misusing them.
- Provide a framework to enable instances of substance misuse by employees in the workplace to be handled in an appropriate, fair, and consistent manner.
- Achieve a balance between supporting employees who come forward with a problem, and the legal requirements to preserve: the health, safety and welfare of employees and others who encounter them, the delivery of high quality and effective services and OLLY's reputation.

This policy is not intended to penalise those taking legitimate medication which may have unforeseen side effects affecting their performance.

Health risks associated with the misuse of intoxicating substances.

While drinking within the governments suggested guidelines has minimal detrimental effect on health, there is several health risks associated with drinking too much alcohol. These include anxiety, sexual difficulties such as impotence, slowed breathing and heartbeat and impaired judgement leading to accidents and injuries. If alcohol is drunk during pregnancy, it can pass through the placenta and damage the foetus. Drinking heavily can also lead to an increased risk of a variety of cancers. Consuming large amounts of alcohol increases blood pressure. This puts a strain on blood vessels and is a major risk for a stroke. Other health risks include osteoporosis (thinning of the bones,) pancreatitis (inflammation of the pancreas), stomach ulcers, heart disease, dementia, and other brain damage. Alcohol is frequently associated with mental health problems.

Further information about the health risks of drinking too much can be found at www.drinkaware.co.uk

DRUGS

Health risks depend on what drugs are taken and can include:

- Increased risks of developing certain cancer.
- Depression and more severe mental health problems.
- Brain damage.
- Vascular disease.

More information can be found on FRANK (www.talktofrank.com)

Responsibilities of Management and Employees

THE ROLE OF THE MANAGER IS:

Drinking alcohol is an accepted part of social life for many people and can be hard for managers to draw a line between acceptable social drinking and alcohol abuse. Similarly recognising the signs of drug abuse can be difficult. It is emphasised that managers are not expected to be experts in this area. Employees with a drunk and/or drug problem may have higher absence levels than their colleagues but this is not always the case. Similarly, performance may not always be adversely affected. Managers therefore have a twofold role in dealing with these issues:

- Where appropriate, to highlight the effect on performance, conduct or attendance.
- To encourage the individual to seek help with their dependence and offer appropriate support.

Advice can be sought before speaking to the individual on a confidential basis.

EMPLOYEES RESPONSIBILITY

- Familiarise themselves with the policy and comply with its provisions.

- Present a professional, courteous, and efficient image to those who they encounter. Therefore, you have a personal responsibility to adopt a responsible attitude towards drinking and taking prescribed and over the counter drugs.
- Where appropriate, co-operate with any arrangements for help and support offered by OLLY/FFFJ to address any drug or alcohol problems you may have.

No employee is under any obligation to accept help and support if it is not appropriate to their circumstances.

CONFIDENTIALITY

OLLY will treat issues relating to dependence, or misuse of, alcohol or drugs in confidence, within limits of what is practicable within the law. To provide effective support and help it may be necessary, for example, for information to be shared with others.

HELP AND SUPPORT

Employees are strongly encouraged to seek help if they have concerns regarding their alcohol and drug consumption.

Where an employee has disclosed, they have a drug and alcohol problem OLLY will always adopt a constructive and supportive approach to assist them and address it.

OUTSIDE WORKING HOURS

- Employees are discouraged from consuming intoxicating substances 12 hours before their working day starts.
- Remember intoxicating substances such as alcohol stay in the system for some time.

CONTROLLED DRUGS

Employees are not permitted to possess, store, trade or sell controlled drugs on OLLY premises or bring OLLY into disrepute by engaging in such activities outside work. Where evidence warrants, OLLY will inform the police of illegal drug use or any activity or behaviour related to drugs or alcohol over where there are concerns of their legality.

Possible Indicators of alcohol or drug misuse:

- Erratic performance
- Unusual irritability or aggression
- Dilated pupils
- Hand tremor
- Increase of risks of accident or near misses.
- Overconfidence
- Inappropriate behaviour
- Sudden mood changes
- Reduced response time
- A tendency to become confused.

- Reduced productivity
- Absenteeism
- Poor timekeeping
- Deterioration in relationships
- Dishonesty and theft
- Financial irregularities

Agencies and Support Mechanisms

- Samaritans – www.samaritans.org
- Cocaine anonymous – www.cauk.org.uk
- Narcotic anonymous – www.ukna.org
- Drinkaware – www.drinkaware.co.uk
- Action on addiction – www.actiononaddiction.org.uk

Families Fighting for Justice and O.L.L.Y (Our Lost Love Years)

Internet Policy

Internet acceptable use policy

Networked resources, including internet access, are potentially available to learners and staff at OLLY/FFFJ. All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and or retrospective investigation of the user's use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of KIND. Any expression of a personal view about OLLY/FFFJ or associates matters in any electronic form of communication must be endorsed to that effect.

Any use of the network that would bring the name of OLLY/FFFJ or associates into disrepute is not allowed.

OLLY/FFFJ expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to learners in the use of such resources. Independent learner users of the internet or will only permitted upon receipt of signed permission and agreement forms as laid out below. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion

CONDITION OF USE

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and learners will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuses of the network to the management.

NETWORK ETIQUETTE AND PRIVACY

Users are expected to abide by the rule of network etiquette. These rules include but are not limited to the following:

1. Be polite – never send or encourage others to send abusive messages
2. Use appropriate language – users should remember that they are representatives of OLLY/FFFJ on a global public system. Illegal activities of any kind are strictly forbidden
3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group
4. Privacy – do not reveal any personal information (e.g home address, telephone number) about yourself or other users. Do not trespass into other user's. Do not trespass into other users' files or folders

INTERNET ACCEPTABLE USE POLICY

1. Password – do not reveal your password to anyone. If you think someone has learned your password then contact Peter Dunning.
2. Electronic mail – is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities Do not send anonymous messages
3. Disruptions – do not use the network in any way that would disrupt use of the network by others.
4. Learners will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them
5. Staff and learners finding unsuitable websites through the KIND network should report the web address to the management.
6. Do not introduce floppy disks or pen drives into the network without having them checked for viruses.
7. Do not attempt to visit websites that might be considered inappropriate. (Such sites visited leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use)
8. Unapproved system utilities and executable files will not be allowed in learners' work areas or attached to e-mail.
9. Files held on the KINDS network will be regularly checked by the staff.
10. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur

UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished

Users finding machines logged on under other users username should log off the machine whether they intend to use it or not

Accessing or creating, transmitting, displaying or publishing any material (e.g images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety

Accessing or creating, transmitting or publishing any defamatory material.

Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data

Transmitting unsolicited material to other users (including those on other networks)

Unauthorised access to data and resources on the KIND network system or other systems

User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere

INTERNET ACCEPTABLE USE POLICY

Additional Guidelines

1. Users must comply with the acceptable use policy of any other networks that they access
2. Users must not download software without approval from staff

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by KIND. KIND will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk

NETWORK SECURITY

Users are expected to inform the management immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network

PHYSICAL SECURITY

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes for example will need to be physically protected by locks and or alarms

WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the KIND system will result in loss of access, disciplinary action and if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

MEDIA PUBLICATIONS

Written permission from parents or carers will be obtained before photographs of learner or published. Named images of learners will only be published with the separate written consent of their parents or carers.

Publishing includes, but is not limited to:

- The OLLY/FFFJ website
- The Local Authority web site,
- Web broadcasting
- TV presentations
- Newspapers

Learners' work will only be published (e.g. photographs, videos, tv presentations, web pages etc) if parental consent has been given

Families Fighting for Justice and O.L.L.Y

(Our Lost Love Years

Managing Allegations of Abuse Against Staff

Reviewed 1st March 2023

It is essential that allegations made against staff including volunteers and placement students are dealt with quickly, fairly, and consistently and in a way that provides effective protection for the child as well as supporting the person who is subject to the allegation.

All staff should be aware of what to do should they receive an allegation against another member of staff or they themselves have concerns about the behaviour of another member of staff. It is our policy that allegations will be reported straight away to the child protection officer. Should the allegation be made against him or in his absence please report it to **Jean Taylor**.

Purpose

The policy will be adopted in respect of allegation that might indicate that a member of staff, volunteer or placement student is not suitable to work with children. If they have:

- Behaved in a way that has harmed a child or may harm a child.
- Possibly created an offence against or related to a child.
- Behaves towards a child or children which indicate they are unsuitable to work with children.

In addition, procedures will also be used if:

- There are concerns about the person's behaviour towards their own child.
- Children unrelated to their employment or voluntary work, and there has been a recommendation from a strategy discussion that consideration should be given to the risk posed to children they work with.
- When an allegation is made about abuse that took place some time ago and the accused person may still be working or having contact with children.

There may be up to three strands of consideration of an allegation.

- A police investigation of a possible criminal offence.

- Enquiries and assessment of children's social care about if a child needs protection or in need of services.
- Consideration by an employer of disciplinary action in respect of the individual.

Supporting those involved

Parents or carers of the child should be told about the allegation as soon as possible if they do not already know. They should be kept informed about the progress of the case and told the outcome if there is not a criminal prosecution. That includes the outcome of any disciplinary process. N.B The deliberations of any disciplinary hearing, and the information considered in reaching a decision, cannot be normally disclosed, but those concerned should be informed of the outcome. IN cases where a child may suffer significant harm, or there may be a criminal prosecution, children's social care or the police as appropriate, should consider what support the child may need.

The employer should also keep the person who is subject to the allegations informed of the progress of the case and arrange to provide appropriate support to the individual while the case is on-going. If the person is suspended the employer should also decide to keep the individual informed about developments in the workplace.

Confidentiality

OLLY's/FFFJ confidentiality should be always adhered to.

Every effort should be made to maintain confidentiality and guard against publicity while an investigation is being investigated/considered. Police will not normally provide any information to the press or media that may identify an individual who is under investigation, unless and until the person is charged with a criminal offence.

Resignations and Compromise Agreements

The fact that a person tenders his or her resignation, or ceases to provide their services, must not prevent an allegation being followed up. It is important that all effort is made to reach a conclusion in all cases of allegations bearing on the safety and well-being of the child. Wherever possible the person should be given a full opportunity to answer the allegation and any supporting evidence and reaching a judgement about whether it can be regarded as substantial on the basis of all the information available should continue even if that cannot be done or the person does not cooperate.

By the same token, so called 'compromise agreements' by which a person agrees to resign, the employer agrees not to pursue disciplinary action, and both parties agree a form of words to be used in any future reference, must not be used in these cases. In any event, such an agreement will not prevent a thorough police investigation where appropriate.

Record Keeping

It is important that employers keep a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and details of any actions taken, and decisions reached on a person's confidential personnel file and a copy given to the individual. Such information should be retained on file, including for people who leave the organisation, at least until

the person reaches normal retirement age or for 10 years if that will be longer. The purpose of the record is to enable accurate information is to be given in response to any request for a reference.

Timescales

It is in everyone's interest to resolve cases as quickly as possible consistent with a thorough and fair investigation. Every effort should be made to manage cases and avoid unnecessary delay.

Initial Considerations

Procedures need to be applied with common sense and judgement. Some allegations may be so serious as to require immediate referral to children's social care and the police for investigation. Others may be less serious and at first sight might not seem to warrant consideration of a police investigation, or enquiries by children's social care. However, it is important to ensure that all allegations are followed up. The employer should inform the accused person about the allegation as soon as possible.

Suspension

The possible risk of harm to children posed by an accused person needs to be effectively evaluated and managed, in respect of the children involved in the allegations, and any other children in the individuals home, work or community life. In some cases that will involve the employer to consider suspending the person. An individual will be immediately suspended whereby the child has suffered significant harm or the allegation warrants a police or children's services investigation.

Families Fighting for Justice and O.L.L.Y
(Our Lost Love Years)
ADMISSIONS POLICY (CHILD)

Reviewed 1st March 2023

Prior to a child attending OLLY/FFFJ their parents/carers are asked to complete a consent form
The information will include the following:

- 1 Name, home address and date of birth of each child
- 2 Daytime/emergency contact phone number
- 3 Any medication the child is on, the dosage and how often is required.
- 4 Does the child have any allergies? If so, what are they?
- 5 Does the child have any disabilities? If so, what are they
- 6 Does the child have any fears or phobias? If so, what are the
- 7 The child's dietary requirements
- 8 Consent to attend centre, any outdoor trips organised by the centre and any medical operative or dental treatment which may be required
- 9 Permission for photographs/moving images to be taken of the child by the OLLY/FFFJ team
- 10
- 11 We also have a behavioural rules part of our admissions policy
- 12 Can the child swim and at what capability?

OLLY/FFFJ Safer Recruitment Policy

The purpose of this policy is to set out the minimum requirements of a recruitment process that aims to:

Attract the best possible applicants to the vacancies.

Deter prospective applicants who are unsuitable to work with children or young people.

Identify and reject applicants who are unsuitable to work with children and young people.

Our designated safeguarding co-ordinator has attended accredited training in safer recruitment to sit on the interview panel.

Inviting applicants

Advertisements for all posts will read the statement:

OLLY/FFFJ is committed to safeguarding children and young people. All post holders are subject to a satisfactory enhanced Criminals Records Bureau check.

Prospective applicants will be supplied, as a minimum, with the following:

- Job description and person specification
- Safeguarding policy
- Safer recruitment policy
- The selection procedure for the post
- An application form.

All prospective applicants must complete an application form in full.

Short listing and references

Short listing of candidates will be against the person specification.

References will be taken up prior to interview.

References will be sought directly from the referee. References or testimonials will never be accepted directly from the candidate.

Where necessary referees will be contacted by telephone or email to clarify any discrepancies. A detailed written note will be kept of these exchanges.

Where necessary previous employers who have not been named as referees will be contacted to clarify any discrepancies. A written detailed note will be kept of these exchanges.

Referees will be asked specific questions about the candidate's suitability for working with children and young people, any disciplinary warnings including time expired warnings that relate to safeguarding children, the candidate's suitability for the post.

Employees are entitled to see and receive, if requested, copies of their employment references.

The Selection processes

Selection techniques will be determined by the nature and duties of the vacant post. But all applicants will require an interview.

Interviews will always be face to face. Telephone interviews may be done at the short-listing stage but will not substitute face to face interviews.

Candidates will always be required: to explain satisfactory gaps in employment, to explain satisfactorily any discrepancies available to recruiters, to declare any information that is likely to appear on a CRB disclosure and to demonstrate their capacity to safeguard and protect the welfare of children and young people.

EMPLOYMENT CHECKS

All successful applicants are required:

- To provide proof of identity
- To complete a DBS Check and receive satisfactory clearance.
- To provide actual certificates of qualifications
- To complete a confidential health questionnaire
- To provide proof of eligibility to live and work in the UK.

Induction

All staff new to OLLY/FFFJ will receive induction training that will include safeguarding and safe working practices. New recruits are given a 6-month probationary period when appointed. During this time, they will have regular meetings with their line manager

Families Fighting for Justice and O.L.L.Y

(Our Lost Love Years)

Office and Surrounding Areas Risk Assessment

Reviewed 1st March 2023

Before any programme commences, an induction will take place where all visitors will be encouraged to inform staff of any potential hazards including breakages and spillages. A daily check of the centre is carried out at the start of every working day, which is recorded on our Daily Checklist.

Potential Hazard	Who might be harmed and why?	Risk Measure	Precaution to be taken	Action carried out by whom
Doors locked	Children and adults – may not be able to escape in the event of fire	Low	Doors to be unlocked in the morning	All staff daily
Plug sockets	Children can put fingers into them	Low	Unused plug sockets to be switched off	All staff daily
Cooker	Children and adults – burns	Low	Children to be supervised at all times when cooking	All staff on activity
Electrical wires e.g. smart board	Anyone – trip hazard	Low	All wires tidied away	All staff on activity
Stairs	Anyone using stairs – trip or fall	Low	Stairwells to be lit appropriately, no objects to be placed on the stairs, no running on the stairs	Staff
Lift	Children/adults – lift may break down, use in fire	Low	Lift will only be used when necessary and the person will be accompanied by a	Staff

			member of staff	
Coat Hooks	Children may bang their heads on them	Low	Children to be supervised at all times and be told in advance how to walk around the centre	Staff
Doors	Children may trap their fingers	Low	Children to be supervised closely at all times	Staff
Glass	Children or adults may trip and bang their heads on the glass	Low	Shoe laces to be fastened at all times. Any objects on the floor must be picked up immediately	Children/staff/visitors
Toilets	Children may slip on any spillages on the floor	Low	Any spillages will be mopped up immediately	Children/staff/visitors
Objects on floors	Children, staff or volunteers may trip over them	Low	Any objects will be picked off the ground immediately	Children/staff/visitors
Hot water	Anyone who comes into contact with the water	Low	Temperature is controlled by a thermostat	Staff
Scissors/glue/paint	Children – not using them correctly, putting glue or paint into their mouth	Low	Children will be supervised at all times	Staff
Knives	Children – by using them inappropriately	Low	Knives are kept in a locked cupboard out of children's reach	Staff
Hot drinks	Children/adults – in the event of spillages	Low	Hot drinks are kept away from the children at all times	Staff/visitors
Pencils	Children – may hurt themselves when they have been sharpened	Low	Children will be supervised closely at all times	Staff
Support pillar	Children – may run into them	Low	Children will be supervised closely at all times and pillars will be highlighted to children before sessions begin	Staff

Surrounding area	Children, staff and visitors – trips or falls if children run around	Low	Children informed of rules. Daily health and safety checks carried out, any dangerous objects removed	All staff
Steps	Children – may trip or fall on them	Low	Children will be told to hold onto the handrail whilst on the steps	All staff

Families Fighting for Justice / O.L.L.Y

EQUALITY AND DIVERSITY

EQUALITY ACT 2010

Families Fighting for Justice and O.L.L.Y believes and recognises that the diversity of people that we work with is a huge asset and is seen as one of our strength. Families Fighting for Justice/O.L.L.Y is committed to providing equality of opportunity and tackling discrimination, harassment, intimidation and disadvantaged. We are also committed to achieving the highest standards in service, delivery, decision making and employment practice.

Families Fighting for Justice and O.L.L.Y will not tolerate less favourable treatment of anyone on the grounds of their sex; • gender reassignment; • marriage and civil partnership; • pregnancy and maternity; • race (including ethnic origin, colour, nationality and national origin); • disability; • sexual orientation; • religion and or belief; and • age, trade union or political activities.

In driving this policy forward we will;

- Seek to ensure that team Families Fighting for Justice/O.L.L.Y is treated fairly during their working time with us
- Take action to eradicate discrimination and inequality when delivering our services
- Evaluate the impact of our policies and services and make changes to them if they impact unfairly on any groups
- Seek to make it possible for our services to be accessible for all who want to use them
- Work with others to stamp out intimidation and harassment.
- Consider the needs of all in the methods we use for communicating with team Families Fighting for Justice/O.L.L.Y and service users.

Families Fighting for Justice/O.L.L.Y is committed to achieving equality all by removing direct and indirect discrimination on the grounds of:

- sex;
- gender reassignment;
- marriage and civil partnership;
- pregnancy and maternity;
- race (including ethnic origin, colour, nationality and national origin);
- disability;
- sexual orientation;
- religion and or belief;
- age.

We will do this by:

- Meeting our responsibilities for all equal opportunities in relevant legislation.

- Making sure our policies, plans, practices and procedures reflect and incorporate equality objectives. Tackling all forms of bullying harassment and intimidation.

Our policy will be monitored and reviewed annually to ensure that equality and diversity is continually promoted in the workplace.

Reviewed on 23rd May 2021

Approved by

Approved by Print Name.....

Witness by.....

Witness by (Print Name)

Families Fighting for Justice and O.L.L.Y

First Aid Policy

Families Fighting for Justice and O.L.L.Y is committed to providing emergency first aid provision to deal with accidents and incidents affecting employees, children, and visitors.

AIMS OF THE POLICY

1. To ensure that we have adequate, safe and effective first aid provision in order for every member for the team Families Fighting for Justice and O.L.L.Y to be well looked after in the event of any illness, accident or injury, no matter how major or minor.
2. To ensure that all staff are aware of the procedures in the event of any illness, accident, or injury.
3. To ensure that medicines are only administered where appropriate permission been granted.
4. To ensure that all medicines are appropriately stored.
5. To promote infection control

Nothing in this policy should affect the ability of any person to contact the emergency services in the event of a medical emergency. For the avoidance of doubt, staff should dial 999 for the emergency services in event of medical emergency before implementing the terms of this policy and make clear arrangements for liaison with ambulance service.

To achieve the Policy Aims, Families Fighting for Justice and O.L.L.Y will:

Have suitably stocked first aid first aid boxes, which are checked weekly.

Carry out suitable and sufficient assessment of the risks posed to persons if they suffer an accident, injury, or ill health.

Ensure that all staff as appropriately First Aid trained.

Provide information to employees and parents on the arrangements for first aid.

Having a procedure for managing accidents, including immediate liaison with emergency services, medical staff, and parents.

Review and monitor arrangements for First Aid as appropriate on a regular basis

First Aid boxes are in the following rooms:

Kitchen

HUB Office

Main Office

Top floor office

First Aid travel bags for off-site visits are in the main office.

OLLY CODE OF CONDUCT

Reviewed 1st March 2023

INTRODUCTION

Welcome to OLLY. The following pages are a statement covering various aspects of your employment at OLLY.

HOURS OF WORK

Your contracted hours will be given in your contract of employment. Time off in lieu of extra hours must be agreed with the OLLY Manager in advance. If you are unable to attend work or are going to be late you must telephone the office as soon as possible on 0151 709 2994.

CONFIDENTIALITY

You must keep all information given to you or always created by you during your employment confidential while you are an employee and after your employment ends. More details are given in our confidentiality Policy.

HEALTH AND SAFETY

You are expected to comply with our current health and safety legislation and be familiar with our Health and Safety Policy

OLLYS PROPERTY

You are expected to take reasonable care of our property issued to you and may be liable for any loss or damage arising from your negligence. You must not remove equipment, furnishing or supplies from the workplace without the permission of the OLLY Manager. Supplies purchased by OLLY must not be used for personal use.

PERSONAL BELONGINGS

OLLY cannot accept any responsibility for your own belongings while you are at work and you should therefore ensure that you only bring with you those items which you will need.

VEHICLES

If your own vehicle is used for OLLY business, regardless of whether you claim reimbursement of petrol costs for this you must ensure that your insurance policy is in force and includes cover for such use. You must also have a current MOT, Road tax and a valid driving licence.

SMOKING

OLLY holds a strict NO SMOKING policy in all offices, grounds, premises, and vehicles.

ACCEPTANCE OF GIFTS

You must never ask or influence any individual or organisation to give you a gift.

PRIVATE TELEPHONE CALLS

You may only make essential private phone calls and must seek permission prior to this.

INTERNET USE

The use of the internet in a manner not conducive with business ethics may expose the individual and KIND to possible danger and fines. You are not permitted to purchase or install third party internet webpage access software or other software devices. **ANY MATERIAL DOWNLOADED THAT COULD BE CONSTRUED AS PORNAGRAPHIC OR OFFENSIVE WILL LEAD TO DISCIPLINARY ACTION**

COMPUTER EQUIPMENT

You must only use computer equipment, systems, and networks relevant to your work unless authorised by the OLLY Manager. There are no circumstances in which you may use OLLYS computers or networks for purposes that are unlawful, offensive or that might bring OLLYS reputation into disrepute. Note that computers and networks may be subject to audits, monitoring and investigations to protect OLLYS assets.

EMAIL

You must only use the email service for OLLY business unless otherwise instructed by the OLLY Manager. Mail on the internet is not secure: never include anything in an email message that you want to keep private and confidential. Do not send threatening emails. Do not send racially, politically, or sexually offensive emails. Do not send out confidential materials outside of OLLY Organisation. Do not participate in chain letters sent out via email. Do not send electric correspondence that may in any way reflect poorly on OLLY, as each transaction can be traced to KIND. Do not open any email attachments unless you are sure of what they contain and where they have come from.

COMMUNICATION

You have a responsibility to read all appropriate communication books, check any message systems in place and inform an appropriate member of staff of any appointments you may be attending before you leave and provide a time you anticipate returning.

PHOTOGRAPHY

Under no circumstances may Team Kind, visitors or parents/carers take still or moving images of children on their mobile phones or cameras for their own personal use.

SOCIAL NETWORKING SITES

Team Kind may never 'add' a child or young person on any social working sites. Children's pictures may not be used on sights without parental/carers permission. Underpinning Principles with accordance to 'Guidance for Safer Working Practice for Adults who works with children and Young People'.

- The welfare of the child is paramount (children Act 1989)
- It is the responsibility of all adults to safeguard and promote the welfare of children and young people. This responsibility extends to a duty of care for those adults employed, commissioned, or contracted to work with children and young adults.
- Adults who work with children are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Adults should work and be seen to work, in any open and transparent way.
- The same professional standards should always be applied and should be sensitive to differences expressed through culture, disability, gender, language, racial origin, religious belief and/or sexual identity.

PERSONAL APPEARANCE

- A t-shirt will be provided for you during your time with us. Remember we are role models and therefore should try and be smartly dressed. We do not recommend large earrings or long hair to be worn out.
- All staff must maintain a high level of personal hygiene.



O.L.L.Y
Our Lost Love Years
Children's Bereavement Charity

Our Lost Love Years

6 Anson Street

Liverpool

L3 5NY

Phone: 0151 709 2994 (9-5pm)

Mobile: 07740 149899

Website: www.ourlostloveyears.co.uk

Email: info@ourlostloveyears.co.uk

BEHAVIOUR RULES

I..... Will adhere to the

Print Name

Behaviour and language rules that are set out below.

1. No Foul Language will be aimed at anyone within our charity
2. No abusive Language to be aimed at anyone within our charity
3. No Threatening or abusive Behaviour towards any member
4. No discussing outside of the building what is heard within our group sessions
5. I will treat all Volunteers and other members with respect

Name

Signed

Dated

Signed by Lead Session Worker

.....

“From little acorns...big oak trees grow”

Charity No: 113 4103

FFFJ/OLLY Anti-Bullying Policy

Review Date 1st March 2023

FFFJ/OLLY is completely opposed to bullying and will not tolerate it. It is entirely contrary to the values and principles we work and live by. All members of the FFFJ/OLLY community have a right to work in a secure and caring environment. They also have a responsibility to contribute, in whatever way they can, to the protection and maintenance of such an environment.

- Children have a right to learn free from intimidation and fear.
- The needs of the victim are paramount.
- FFFJ/OLLY will not tolerate bullying behaviour.
- Bullied children will be listened to.
- Reported incidents will be taken seriously and thoroughly investigated.

Definition of Bullying

Bullying is an act of aggression, causing embarrassment, pain or discomfort to someone. It can take a number of forms; physical, verbal, making gestures, extortion and exclusion. It is an abuse of power. It can be planned and organised, or it may be unintentional. It may be perpetrated by individuals or by groups of people.

Forms of Bullying

- Physical violence such as hitting, pushing or spitting at another pupil.
- Interfering with another pupil's property, by stealing, hiding or damaging it.
- Using offensive names when addressing another person.
- Teasing or spreading rumours about another person or his/her family.
- Belittling another child's abilities or achievements.
- Writing offensive notes or graffiti about another person.
- Excluding another child from a group activity.
- Ridiculing another child's appearance, way of speaking or personal mannerisms.
- Misusing technology (internet or mobiles) to hurt or humiliate another person.

The responsibilities of Staff

Our staff will:

- Foster in our children self-esteem, self-respect and respect for others.
- Demonstrate by example the high standards of personal and social behaviour we expect of our children.
- Discuss bullying, so that every child learns about the damage it causes to both the child who is bullied and to the bully, and the importance of telling a member of staff about bullying when it happens.
- Be alert to signs of distress and other possible indications of bullying.
- Listen to children who have been bullied, take what they say seriously and act to support and protect them.

- Follow up any complaint by a parent about bullying and report back promptly and fully on the action which has been taken.
- Deal with observed instances of bullying promptly and effectively, in accordance with agreed procedures.

The responsibilities of OLLY

We expect them to:

- Refrain from becoming involved in any kind of bullying, even at the risk of incurring temporary unpopularity.
- Intervene to protect the child who is being bullied, unless it is unsafe to do so.
- Report to a member of staff any witnessed or suspected instances of bullying, to dispel any climate of secrecy and help to prevent further instances. Anyone who becomes the target of bullies should:
 - Not suffer in silence, but have the courage to speak out, to put an end to their own suffering and that of other potential targets.

The responsibilities of parents

We ask our parents to support their children and OLLY by:

- Watching for signs of distress or unusual behaviour in their children, which might be evidence of bullying.
- Advising their children to report any bullying to a member of staff and explain the implications of allowing the bullying to continue unchecked, for themselves and for others.
- Advising their children not to retaliate violently to any forms of bullying.
- Being sympathetic and supportive towards their children and reassuring them that appropriate action will be taken.
- Keeping a written record of any reported instances of bullying.
- Informing the staff of any suspected bullying, even if their children are not involved.
- Co-operating with OLLY, if their children are accused of bullying, try to ascertain the truth. And point out the implications of bullying, both for the children who are bullied and for the bullies themselves.

The responsibilities of all

Everyone should:

- Work together to combat and, hopefully in time, to eradicate bullying.

Guidelines for records and sanctions

Procedures for dealing with incidents of bullying behaviour (Includes steps taken to support and respond to the needs of both bullied and bullying children).

- Steps taken to support and respond to the needs of both bullied and bullying children:
- Records kept:

- Action which may be taken:
- Contacting parents/carers of all pupils concerned in the bullying incident:
- Feedback to those concerned:
- Sanctions:

Continuous professional development of staff.



LIVERPOOL SAFEGUARDING CHILDREN BOARD

Safeguarding - Basic Awareness

HANDOUT PACK

Attendees are requested to print and bring this handout pack to support delivery of the session

Name: _____

Liverpool Safeguarding Children Board

Safeguarding - A Basic Awareness

Thank you for your interest to attend the Basic Safeguarding course delivered on behalf of the Liverpool Safeguarding Children Board.

This is a **half day** course for staff from all agencies who are involved in work with children and families; either in a statutory or voluntary capacity that work with or come into contact with children and young people and their families.

Morning sessions are delivered from 9.30am – 12.30pm with registration at 9.15am

Afternoon sessions are delivered from 1.30pm – 4.30pm with registration at 1.15pm

The course aims to provide staff with a basic understanding of Liverpool Safeguarding Children and Young people procedures and system and gives workers an introduction to issues of recognition of the different categories of child abuse. *It is therefore not appropriate for workers who have substantial experience of working in the child protection system.*

PLEASE NOTE: This session DOES NOT COVER safeguarding adults

Learning Outcomes

Through discussion, scenario review and group working attendees will develop an understanding as to the importance of their role in the safeguarding of children and understand the background to safeguarding and the legislations that underpin current safeguarding requirements.

The session aims to enable attendees to develop awareness as to what constitutes child abuse, the effects of child abuse and how that abuse may be recognised.

Importantly it will enable workers to be secure in their understanding of 'what to do' and who to contact if they are concerned for the welfare of a child or young person or where a child is at risk of suffering harm

Safeguarding - Basic Awareness

'Safeguarding Children & Young People'

Programme

9.15 Arrival / Signing in / Coffee

9.30 Welcome and Introductions

Safeguarding - Context

Definitions of Abuse

Child Abuse: Indicators / Effects

Break

Responding to Need Guidance and Levels of Need Framework

Early Help

What to do if you are concerned for the welfare of a child

Safer Working Practices

Evaluations

12.30 Summary and Close

Definitions of Abuse

Safeguarding - Glossary

Child

Anyone who has not yet reached their 18th birthday. The fact that a child has reached 16 years of age, is living independently or is in further education, is a member of the armed forces, is in hospital or in custody in the secure estate, does not change his/her status or entitlements to services or protection.

Safeguarding and promoting the welfare of children

Defined for the purposes of this guidance as:

- protecting children from maltreatment;
- preventing impairment of children's health or development;
- ensuring that children are growing up in circumstances consistent with the provision of safe and effective care; and
- taking action to enable all children to have the best life chances.

Child protection

Part of safeguarding and promoting welfare. This refers to the activity that is undertaken to protect specific children who are suffering, or are likely to suffer, significant harm.

Abuse

A form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm, or by failing to act to prevent harm. Children may be abused in a family or in an institutional or community setting by those known to them or, more rarely, by others (e.g. via the internet). They may be abused by an adult or adults, or another child or children.

Physical abuse

A form of abuse which may involve hitting, shaking, throwing, poisoning, burning or scalding, drowning, suffocating or otherwise causing physical harm to a child. Physical harm may also be caused when a parent or carer fabricates the symptoms of, or deliberately induces, illness in a child.

Emotional abuse

The persistent emotional maltreatment of a child such as to cause severe and persistent adverse effects on the child's emotional development. It may involve conveying to a child that they are worthless or unloved, inadequate, or valued only insofar as they meet the needs of another person. It may include not giving the child opportunities to express their views, deliberately silencing them or 'making fun' of what they say or how they communicate. It may feature age or developmentally inappropriate expectations being imposed on children. These may include interactions that are beyond a child's developmental capability, as well as overprotection and limitation of exploration and learning, or preventing the child participating in normal social interaction. It may involve seeing or hearing the ill-treatment of another. It may

involve serious bullying (including cyber bullying), causing children frequently to feel frightened or in danger, or the exploitation or corruption of children. Some level of emotional abuse is

involved in all types of maltreatment of a child, though it may occur alone.

Sexual abuse

Involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example, rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse (including via the internet). Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children.

Neglect

The persistent failure to meet a child's basic physical and/or psychological needs, likely to result in the serious impairment of the child's health or development. Neglect may occur during pregnancy as a result of maternal substance abuse. Once a child is born, neglect may involve a parent or carer failing to:

- provide adequate food, clothing and shelter (including exclusion from home or abandonment);
- protect a child from physical and emotional harm or danger;
- ensure adequate supervision (including the use of inadequate care-givers); or ensure access to appropriate medical care or treatment.

It may also include neglect of, or unresponsiveness to, a child's basic emotional needs.

Young carers

Are children and young people who assume important caring responsibilities for parents or siblings, who are disabled, have physical or mental ill health problems, or misuse drugs or alcohol.

Early Help

Providing early help is more effective in promoting the welfare of children than reacting later. Early help means providing support as soon as a problem emerges, at any point in a child's life, from the foundation years through to the teenage years.

Effective early help relies upon local agencies working together to:

- identify children and families who would benefit from early help;
- undertake an assessment of the need for early help; and
- provide targeted early help services to address the assessed needs of a child and their family which focuses on activity to significantly improve the outcomes for the child. Local

authorities, under section 10 of the Children Act 2004, have a responsibility to promote inter-agency cooperation to improve the welfare of children.

Working Together 2015

Responding to Need Guidance and Levels of Need Framework

Liverpool Safeguarding Children Board's (LSCB) 'Responding to Need Guidance' has been designed with partners from across the Children's Trust and the LSCB to ensure that children's needs are responded to at an appropriate level and in a timely way. The guidance should be seen as overarching guidance for the whole of the children and young people's workforce within Liverpool. It is a guide for all agencies, professionals and volunteers, to consider how best to meet the needs of individual children. Individual agency response to levels of needs will vary depending on the individual agency but their responses should all support this framework, and deliver appropriate interventions for children and families.

PARTNERSHIPS AND JOINT WORKING ARE KEY TO ENSURING POSITIVE OUTCOMES FOR CHILDREN, AND TO REDUCE THE NEED FOR MORE INTENSE INTERVENTIONS AT A LATER STAGE.

The Early Help Assessment is the agreed framework that supports partnerships/joint working and multi-agency interventions which are recorded on the Early Help Assessment Tool documentation (EHAT).

This framework follows the 'windscreen model' which illustrates when services begin from early help to statutory intervention. The aim is that as far as possible, children's needs should be met within universal provision, but where additional needs are identified, flexible support should be introduced at the earliest opportunity, with parental [and/or child where age appropriate] consent, thus alleviating problems that have started to emerge, prevent problems from escalating and help to improve outcomes.

In some circumstances, a child's and family's needs and levels of concern may not be met through coordinated early help, and consequently there may be need to provide more intensive or specialist support lead by social care. The term 'step up' is often used to describe this process.

Equally, the term 'step down' is used to describe children and families moving from a high level of intervention, including statutory intervention, to a lower level of coordinated support. This is important in ensuring that issues do not re-escalate.

Where you have a concern about the welfare of a child or young person - You must review the Responding to Need Guidance and Levels of Need Framework to determine the most appropriate action in response to your concern.

Where your concerns are at level four you should make a referral to Careline.

Careline is Liverpool City Council's 24/7 social care call centre, providing a central contact point for enquiries about services for children, adults, homeless families and people with mental health problems.

Careline: 0151 233 3700

All referrals about the safety or welfare of a child or young person MUST be made to Careline using the Multi Agency Referral form (MARF) unless an EHAT is in place in which case that should be used to 'step up' the concerns.

MARF available at MARF REFERRAL



Universal Services (available at any stage)

Effective Information Sharing

Contact Careline immediately for concerns that a child has suffered or is likely to suffer significant harm. (Level 4) or where you are not certain.

The windscreen model is used for illustration only and does not necessarily reflect the proportions of families within Liverpool that under the level of needs described. Consent is always the needed when offering single or multi-agency support to families and parental engagement is fundamental. This enables effective sharing of information and appropriate support being put in place regardless of the level of need. However, consent is not needed when there are significant welfare concerns or likely risk/harm for a child.

Summary of Learning Outcomes

Have an understanding of what is meant by 'Safeguarding'.	
Have an understanding of the reasons for and the importance of safeguarding children.	
Have an understanding of Early Help and the importance of offering support as soon as a problem emerges	
Have an understanding of the legislation that underpins the safeguarding of children	
Have an understanding of how child abuse may be recognised and the effects of child abuse.	
Know what to do and who to contact when you have concerns, when child abuse is suspected or a child is at risk of harm.	
Know how to make a referral using the Multi agency Referral Form (MARF)	
Understand what is meant by 'disclosure' and know what to do if a child makes a disclosure.	
Know where to go to get further help or advice if I have worries or concerns about the safety or welfare of a child.	
Understand what is meant by 'Safe Professional Conduct' and how this should influence your professional practice.	

Liverpool Safeguarding Children Board (LSCB) is required to evidence how your attendance at today's training impacts upon practice and therefore improves outcomes for children and young people.

We would be grateful if you would identify two (or more) actions that you will undertake in your setting.

LSCB may contact you in the future regarding these actions and outcomes.

N. Walsh LSCB

ACTIONS SHEET

Name: _____ Date Attended: _____

Having attended a Level 1 / Basic Safeguarding Awareness course I intend to:

Action 1:

Action 2:

Please ensure the above actions are recorded on your course evaluation sheet.

OLLY/FFFJ SUN SAFETY PROCEDURE/POLICY

Policy aim:

The aim of the sun safety policy is to protect any member of team OLLY/FFFJ from skin damage caused by the effect of ultraviolet radiation from the sun.

The main elements of this policy are:

- Protection: providing an environment that enables children, young people, volunteers and staff to stay safe in the sun.
- Education: learning about sun safety to increase knowledge and influence behaviour.
- Partnership: working with parents/carers and the wider community to reinforce awareness about sun safety and promote a healthy environment.

At OLLY/FFFJ we feel the children and young people have the right to work outside in a safe environment. Working in our surrounding gardens is an important part of both our day-to-day routine and to our curriculum. We depend on our natural environment in order to teach the children and young people what can be found around them and what we need to protect/enjoy.

As part of the Sun Safety policy we will:

- Encourage the children and young people to wear clothes that provide good sun protection e.g. clothes that cover their bodies and hats to cover their heads and necks.
- Hold outdoor activities in areas of shade whenever possible, and encourage children and young people to use shady areas during lunch times.
- Encourage parents/carers to act as good role models by asking them to pre-apply sun block and appropriate clothing including hats.
- OLLY/FFFJ will ensure the availability of sun hats and sun block to use where permission has been granted.
- Make sure the Sun Safety policy is working and is relevant to the environment we are working in. We will regularly monitor our curriculum, assess shade provision and review the sun safety behaviour of our children, young people and staff.

Good practice to help cope with hot weather.

- Hats are to be worn when outside.
- Sun cream to be applied according to guidelines when parental/carer permission is given.
- Staff should encourage the drinking of water and ensure water is available at regular intervals in order to avoid dehydration.
- Where necessary windows and doors should be opened in order to provide a thorough breeze.
- Staff must ensure that they are setting an example – sensible clothing, drinking plenty of water and taking any required precautions against the high temperature.
-

Heatstroke

Staff should be aware extreme heat can cause heatstroke. Symptoms to look out for are:

- Cramp in arms, legs or stomach
- Feeling of mild confusion or weakness

If anyone has these symptoms, they should find a cool place to rest and be given plenty of fluids. If symptoms get worse or don't go away medical advice should be sought. NHS Direct is available on 08454647

Certification on the rules of OLLY

(Our Lost Love Years).

Any parents/guardians/carers or any family member to a child attending any sessions days out or trips away with OLLY must always adhere to these rules and regulations:

- 1) There must be no foul language used.
- 2) There must never be any discrimination or victimization, slanderers remarks, or false allegations made against OLLY or the charity itself.
- 3) There must not be any slanderers remarks or false allegations directed towards any session worker/volunteer or a member of OLLY or the charity.
- 4) On the day trips out on any sessions that OLLY holds, priority must be given to the children on our minibus pick up service, if the child suffers from ADHD that child will be allowed to have their mother take up a seat, the bus holds 11 seats for children as we have the driver and 2 session workers on board.
- 5) Any seat that is given to an adult is at the discretion of the main session worker.
- 6) OLLY and the charity have a complaints procedure of which the charity is adhered to follow.
- 7) Anyone volunteering for OLLY that has been sent by the job centre or another organisation dealing with volunteers it is the discretion of the charity if they wish to continue with that volunteer, a reason does not have to be given other than not suitable.
- 8) If anyone who has signed the confidentiality act agreement under the act that discloses any information regarding the charity, members, volunteers or the founder or the charity the charity will seek legal action.
- 9) If there are any slanderers remarks that would be a direct discrimination against the charity, the founder or any volunteer working within the charity that could be put out on social media we will pursue this against the writer through a solicitor and the social media network complaints team and that person will be dealt with within the law.
- 10) OLLY will never say a child cannot attend the session if their parent/guardian/carer has acted in a manner that has resulted in them not being allowed to travel on the minibus or attend any OLLY session trips out or breaks away, we will never discriminate against a child belonging to that family and the child will be offered when available a place on the bus to attend the sessions.

The above rules will always be adhered to by those that make themselves present within the charity.

Signed.....

Print Name:.....

Witnessed by:

Signed:.....

Print Name:.....

Key Points

Most volunteer involving organisations hold information on their staff, volunteers and perhaps their clients. This information is likely to be personal data, and therefore subject to the 1998 Data Protection Act which, gives rights to Data Subjects (the people whose data you have) and creates a framework of good practice for those holding personal data. If you collect and hold personal data on individuals then you are legally required to comply with the Act.

What is the Data Protection Act?

The Data Protection Act 1998 regulates the collection, storage, use and disclosure of information about individuals by organisations. Any organisation that keeps information about individuals must comply with the act.

Data Protection Principles

Eight principles are defined to ensure that all "personal data" is handled properly. The act states that the data must be:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

All employees paid/unpaid must conform in accordance to these principles.

Under S.51 (1) It shall be the duty of the Commissioner to promote the following of good practice by data controllers and, in particular, so to perform his functions under this Act as to promote the observance of the requirements of this Act by data controllers.

Under Schedule 5 (1) the corporation sole by the name of the Data Protection Registrar established by the Data Protection Act 1984 shall continue in existence by the name of the [Information Commissioner].

Why is following these principles important?

Failure to observe these principles puts the professional reputation of your organisation at risk. Good information handling enhances your organisation's reputation by increasing member, customer and partner confidence in the organisation. Data protection is the responsibility of all members as well as all staff and agency or contract employees.

Storing of Records

Some guidelines for good practice:

- Compile and Label Files carefully
- All sensitive and confidential data should be locked away and access to the keys strictly controlled
- Keep a log of who has accessed the cabinet where all sensitive and confidential data is kept
- If files are to be stored long term then arrangements need to be made for the keys to be passed from outgoing staff to their successors.
- Access to records need to be limited to people in named roles who either need to know about the information in those records and/or who manage the records/files
- All keys must be returned and accounted for at the end of the day
- All employees paid/unpaid MUST sign for any information they take out of the cabinets

Determining which records should be stored

- What records will we keep and for what purpose?
- Is our record keeping in line with the data protection principles
- How long should we retain information for?
- What is the format of the record
- How will the records be stored and who will have access to them?

Confidentiality

Confidential information is that which is regarded as personal. It is information which is told to an individual, or a group of people, and is not meant for public or general knowledge. It is the duty of volunteers not to reveal to any other person, outside the specifically expressed person within the organisation, any matter which becomes known to the individual via their involvement with the organisation. This includes information which may be traced back to the individual by identifying them or anyone else involved with them. Volunteers are bound by our organisations confidentiality agreement which all volunteers must sign.

Procedure for accessing confidential files

- Sign for keys on the key signing sheet
- Must record the reason for accessing files
- All records for accessing files will be checked, and anybody accessing confidential files without the correct authorisation will be instantly dismissed.

What we expect from our volunteers

We expect all volunteers will adhere to the policies and rules laid out in the above sections. All volunteers will also be expected to comply with the confidential agreement they signed, failing to do so, is an offence under Section 47 (2) of the Data Protection Act 1998. Every volunteer must act in a way which enhances the reputation of both charities at all times, and must never act in a way which would reflect poorly upon our charities or affect our reputation in a negative way.



Families Fighting for Justice
6 Anson Street
Liverpool
L3 5NY
Tel: 0151 709 2994 / 0151 238 1900
www.familiesfightingforjustice.com

Families Fighting for Justice and
O.L.L.Y (Our Lost Love Years)
protects all its
member's data conforming
to the guidelines
laid out in the
Data Protection Act 1998.



**Disclosure
and Barring
Service
(DBS)
checks
(previously
CRB checks)**

DBS

1. Overview

The Criminal Records Bureau (CRB) and the Independent Safeguarding Authority (ISA) have merged to become the Disclosure and Barring Service (DBS). CRB checks are now called DBS checks.

A DBS check may be needed for:

- certain jobs or voluntary work, eg working with children or in healthcare
- applying to foster or adopt a child

Who can ask for a DBS check

An employer can ask for a DBS check for certain roles.

DBS eligibility guidance lists most roles that are eligible for a check. However, the guidance isn't comprehensive so contact DBS if unsure.

Applicants (job candidates) can't do a criminal records check on themselves. Instead, they can request a 'basic disclosure' from Disclosure Scotland (you don't have to be from Scotland to do this).

How to get a DBS check

1. The employer gets an application form from DBS or an umbrella body (a registered body that gives access to DBS checks).
2. The employer gives the applicant the form to fill in and return to them along with documents proving their identity.
3. The employer sends the completed application form to DBS or their umbrella body.
4. DBS sends a certificate to the applicant. The employer has to ask the applicant to see the certificate.

If the applicant has subscribed to the DBS update service, the employer can check their certificate online.

Types of criminal records check

There are 3 types of check. The employer or organisation running the check should provide the applicant with more information about the level of check required.

Criminal record check applicants must be 16 or over.

Standard (£26)

This checks for spent and unspent convictions, cautions, reprimands and final warnings, and will take about 2 weeks.

Enhanced (£44)

This includes the same as the standard check plus any additional information held by local police that's reasonably considered relevant to the workforce being applied for (adult, child or 'other' workforce). It takes about 4 weeks.

'Other' workforce means those who don't work with children or adults specifically, but potentially both, eg taxi drivers. In this case, the police will only release information that's relevant to the post being applied for.

Enhanced with list checks (£44)

This is like the enhanced check, but includes a check of the DBS barred lists, and takes about 4 weeks.

An employer can only ask for a barred list check for specific roles. It's a criminal offence to ask for a check for any other roles.

Volunteers

Checks for eligible volunteers are free of charge. This includes anyone who spends time helping people and is:

- not being paid (apart from for travel and other approved out of pocket expenses)
- not only looking after a close relative

An employer can only apply for a check if the job or role is eligible for one. They must tell the applicant why they're being checked and where they can get independent advice.

A DBS check has no official expiry date. Any information included will be accurate at the time the check was carried out. It is up to an employer to decide if and when a new check is needed.

Applicants and employers can use the [DBS update service](#) to keep a certificate up to date or carry out checks on a potential employee's certificate.

2. Documents the applicant must provide

The Criminal Records Bureau (CRB) and the Independent Safeguarding Authority (ISA) have merged into the Disclosure and Barring Service (DBS). CRB checks are now called DBS checks.

The person going through a DBS check (the applicant) must give their employer original documents (not copies) to prove their identity.

The documents needed will depend on the route the application takes. The applicant must try to provide documents from Route 1 first.

Route 1

The applicant must be able to show:

- 1 document from Group 1, below
- 2 further documents from either Group 1, or Group 2a or 2b, below

At least 1 of the documents must show the applicant's current address.

Route 2

If the applicant doesn't have any of the documents in Group 1, then they must be able to show:

- 1 document from Group 2a
- 2 further documents from either Group 2a or 2b

At least one of the documents must show the applicant's current address. The organisation conducting their ID check must then also use an appropriate external ID validation service to check the application.

Route 3

Route 3 can only be used if it's impossible to process the application through Routes 1 or 2.

For Route 3, the applicant must be able to show:

- a birth certificate issued after the time of birth (UK and Channel Islands)
- 1 document from Group 2a
- 3 further documents from Group 2a or 2b

At least one of the documents must show the applicant's current address. If the applicant can't provide these documents they may need to be fingerprinted.

Continuation sheets

The applicant can [download a DBS continuation sheet](#) for additional information they can't fit on the DBS application form.

Unusual addresses

The applicant must make sure they fill in the address part of the form correctly if they have an unusual address, eg if they live abroad, in student accommodation or a hostel.

Group 1: Primary identity documents

Document	Notes
Passport	Any current and valid passport
Biometric residence permit	UK

Document	Notes
Current driving licence – photocard with paper counterpart	UK, Isle of Man, Channel Islands and EU (full or provisional)

Birth certificate - issued at time of birth	UK and Channel Islands – including those issued by UK authorities overseas, eg embassies, High Commissions and HM Forces
---	--

Adoption certificate	UK and Channel Islands
----------------------	------------------------

Group 2a: Trusted government documents

Document	Notes
Current driving licence – photocard (if you were issued a paper counterpart but don't give it to your checker)	All countries (full or provisional)
Current driving licence – paper version	UK, Isle of Man, Channel Islands and EU (full or provisional)
Birth certificate – issued after time of birth	UK and Channel Islands

Document	Notes
Marriage/civil partnership certificate	UK and Channel Islands
HM Forces ID card	UK
Firearms licence	UK, Channel Islands and Isle of Man

All driving licences must be valid.

Group 2b: Financial and social history documents

Document	Notes	Issue date and validity
Mortgage statement	UK or EEA	Issued in last 12 months
Bank or building society statement	UK and Channel Islands or EEA	Issued in last 3 months

Document	Notes	Issue date and validity
Bank or building society account opening confirmation letter	UK	Issued in last 3 months
Credit card statement	UK or EEA	Issued in last 3 months
Financial statement, eg pension or endowment	UK	Issued in last 12 months
P45 or P60 statement	UK and Channel Islands	Issued in last 12 months
Council Tax statement	UK and Channel Islands	Issued in last 12 months
Work permit or visa	UK	Valid up to expiry date

Document	Notes	Issue date and validity
Letter of sponsorship from future employment provider	Non-UK or non-EEA only - valid only for applicants residing outside of the UK at time of application	Must still be valid
Utility bill	UK – not mobile telephone bill	Issued in last 3 months
Benefit statement, eg Child Benefit, Pension	UK	Issued in last 3 months
Central or local government, government agency, or local council document giving entitlement, eg from the Department for Work and Pensions, the Employment Service, HMRC	UK and Channel Islands	Issued in last 3 months
EU National ID card	-	Must still be valid
Cards carrying the PASS accreditation logo	UK and Channel Islands	Must still be valid

Document	Notes	Issue date and validity
Letter from head teacher or college principal	UK - for 16 to 19 year olds in full time education - only used in exceptional circumstances if other documents cannot be provided	Must still be valid

4. Tracking the application and getting a certificate

The Criminal Records Bureau (CRB) and the Independent Safeguarding Authority (ISA) have merged into the Disclosure and Barring Service (DBS). CRB checks are now called DBS checks.

The person being given a DBS check (the applicant) can check on the progress of their application using the [DBS tracking service](#).

Employers can [track multiple applications](#) and order blank application forms online.

The applicant, employer and organisation that applied for the search will see the results of the check.

You can't access the [DBS update service](#) through the tracking service.

DBS certificate

Once the check is completed, DBS will send a certificate listing the results to the applicant. The employer will have to ask the applicant to [see the certificate](#).

Security features

Certificates have security features to prove they're genuine, including:

- a 'crown seal' watermark repeated down the right side, visible both on the surface and when held up to the light

- a background design featuring the word 'Disclosure', which appears in a wave-like pattern across both sides of a certificate; the pattern's colour alternates between blue and green on the reverse
- ink and paper that change colour when wet

The security features for a CRB certificate issued before 1 December 2012 are the same as for the DBS certificate.

Reusing a DBS check

A DBS certificate only contains information from a DBS check on a certain date and for a particular purpose.

Employers can accept a previously issued certificate but must:

- check the applicant's identity matches the details on the certificate
- check the certificate is of the right level and type for the role applied for
- carry out a free-of-charge status check to see if new information has come to light since the certificate's issue; the applicant must have already joined the DBS update service

Employers can accept a previously issued certificate without a status check but at their own risk.

CRB-branded certificates should be treated the same as DBS-branded certificates.

Lost certificates

DBS can't provide replacements for lost or destroyed certificates.

5. DBS barred lists

The Criminal Records Bureau (CRB) and the Independent Safeguarding Authority (ISA) have merged into the Disclosure and Barring Service (DBS). CRB checks are now called DBS checks.

Jobs that involve caring for, supervising or being in sole charge of children or adults may require an enhanced DBS check with a check of the barred lists.

This will check whether someone's included in the 2 DBS 'barred lists' (previously called ISA barred lists) of individuals who are unsuitable for working with:

- children
- adults

People on the barred lists can't do certain types of work.

There are specific rules for working in places where there are children - known as working in a regulated activity with children.

These are different than the rules for regulated activities for adults.

Refer someone to DBS

Contact the barring helpline for help referring someone to DBS.

DBS barring helpline

Telephone: 01325 953795

Find out about call charges

Employers must refer someone to DBS if they:

- sacked them because they harmed someone
- sacked them or removed them from working in regulated activity because they might have harmed someone
- were planning to sack them for either of these reasons, but they resigned first

You're breaking the law if you don't refer someone to DBS when you should.

Guide to the

General Data Protection

Regulation (GDPR)

Introduction	3
What's new	4
Key definitions	8
Principles	10
Lawful basis for processing	11
Consent	21
Contract	26
Legal obligation	30
Vital interests	34
Public task	37
Legitimate interests	41
Special category data	47
Criminal offence data	50
Individual rights	52
Right to be informed	53
Right of access	61
Right to rectification	71
Right to erasure	77
Right to restrict processing	83
Right to data portability	89
Right to object	100
Rights related to automated decision making including profiling	107
Accountability and governance	114
Contracts	124
Documentation	129
Data protection by design and default	134
Data protection impact assessments	146
Data protection officers	153
Codes of conduct	161
Certification	164
Guide to the data protection fee	167
Security	168
International transfers	181
Personal data breaches	184
Exemptions	192
Applications	193
Children	194

Introduction

Introduction

The Guide to the GDPR explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection.

This is a living document and we are working to expand it in key areas. It includes links to relevant sections of the GDPR itself, to other ICO guidance and to guidance produced by the EU's Article 29 Working Party. The Working Party includes representatives of the data protection authorities from each EU member state, and the ICO is the UK's representative.

Alongside the Guide to the GDPR, we have produced a number of tools to help organisations to prepare for the GDPR:

Further Reading

 [GDPR: 12 steps to take now](#) 

External link

 [Data protection self assessment toolkit](#)

For organisations

What's new

We will update this page monthly to highlight and link to what's new in our Guide to the GDPR.

May 2018

We have expanded our guidance on [data protection by design and default](#), and published detailed guidance on [automated decision-making and profiling](#).

We have published a new page on [codes of conduct](#), and a new page on [certification](#).

We have published [detailed guidance on the right to be informed](#).

We have published detailed guidance on [Data Protection Impact Assessments \(DPIAs\)](#).

We have expanded the pages on the [right of access](#) and the [right to object](#).

We have published detailed guidance on [consent](#).

We have expanded the page on the [right to data portability](#).

April 2018

We have expanded the page on [Accountability and governance](#).

We have expanded the page on [Security](#).

We have updated all of the lawful basis pages to include a link to the [lawful basis interactive guidance tool](#).

March 2018

We have published [detailed guidance on DPIAs for consultation](#). The consultation will end on 13 April 2018. We have also updated the [guide page on DPIAs](#) to include the guide level content from the detailed guidance.

We have published [detailed guidance on legitimate interests](#).

We have expanded the pages on:

- [Data protection impact assessments](#)
- [Data protection officers](#)
- [The right to be informed](#)
- [The right to erasure](#)
- [The right to rectification](#)
- [The right to restrict processing](#)

February 2018

The consultation period for the Article 29 Working party guidelines on consent has now ended and comments are being reviewed. The latest timetable is for the guidelines to be finalised for adoption on 10-11 April.

The consultation period for the Article 29 Working Party guidelines on transparency has now ended.

Following the consultation period, the Article 29 Working Party has adopted final guidelines on [Automated individual decision-making and Profiling](#) and [personal data breach notification](#). These have been added to the Guide.

We have published our [Guide to the data protection fee](#).

We have updated the page on [Children](#) to include the guide level content from the [detailed guidance on Children and the GDPR](#) which is out for public consultation.

January 2018

We have published [more detailed guidance on documentation](#).

We have expanded the page on [personal data breaches](#).

We have also added four new pages in the lawful basis section, covering [contract](#), [legal obligation](#), [vital interests](#) and [public task](#).

December 2017

We have published [detailed guidance on Children and the GDPR](#) for public consultation. The consultation closes on 28 February 2018.

The sections on [Lawful basis for processing](#) and [Rights related to automated individual decision making including profiling](#) contain new expanded guidance. We have updated the section on [Documentation](#) with additional guidance and documentation templates. We have also added new sections on legitimate interests, special category data and criminal offence data, and updated the section on consent.

The Article 29 Working Party has published the following guidance, which is now included in the Guide.

- [Consent](#)
- [Transparency](#)

It is inviting comments on these guidelines until 23 January 2018.

The consultation for the Article 29 Working Party guidelines on breach notification and automated decision-making and profiling ended on 28 November. We are reviewing the comments received together with other members of the Article 29 Working Party and expect the guidelines to be finalised in early 2018.

November 2017

The Article 29 Working Party has published [guidelines on imposing administrative fines](#).

We have replaced the Overview of the GDPR with the Guide to the GDPR. The Guide currently contains similar content to the Overview, but we have expanded the sections on Consent and Contracts and Liabilities on the basis of the guidance on these topics which we have previously published for consultation.

The Guide to the GDPR is not yet a finished product; it is a framework on which we will build upcoming GDPR guidance and it reflects how future GDPR guidance will be presented. We will be publishing more detailed guidance on some topics and we will link to these from the Guide. We will do the same for

guidelines from the Article 29 Working Party.

October 2017

The Article 29 Working Party has published the following guidance, which is now included in our overview.

- [Breach notification](#)
- [Automated individual decision-making and Profiling](#)

The Article 29 Working Party has also adopted guidelines on administrative fines and these are expected to be published soon.

In the [Rights related to automated decision making and profiling](#) we have updated the next steps for the ICO.

In the [Key areas to consider](#) we have updated the next steps in regard to the ICO's consent guidance.

The deadline for responses to our draft GDPR guidance on contracts and liabilities for controllers and processors has now passed. We are analysing the feedback and this will feed into the final version.

September 2017

We have put out for consultation our draft GDPR guidance on contracts and liabilities for controllers and processors.

July 2017

In the [Key areas to consider](#) we have updated the next steps in regard to the ICO's consent guidance and the Article 29 Working Party's Europe-wide consent guidelines.

June 2017

The Article 29 Working Party's consultation on their [guidelines on high risk processing and data protection impact assessments](#) closed on 23 May. We await the adoption of the final version.

May 2017

We have updated our [GDPR 12 steps to take now document](#).

We have added a [Getting ready for GDPR checklist to our self-assessment toolkit](#).

April 2017

We have published our [profiling discussion paper for feedback](#).

March 2017

We have published our [draft consent guidance for public consultation](#).

January 2017

Article 29 have published the following guidance, which is now included in our overview:

- [Data portability](#)
- [Lead supervisory authorities](#)

- [Data protection officers](#)

Key definitions

Who does the GDPR apply to?

- The GDPR applies to 'controllers' **and** 'processors'.
- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.
- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Further Reading

 [Relevant provisions in the GDPR - Articles 3, 28-31 and Recitals 22-25, 81-82](#) 

External link

What information does the GDPR apply to?

• **Personal data**

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

• **Sensitive personal data**

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Further Reading

 [Relevant provisions in the GDPR - Articles 2, 4, 9, 10 and Recitals 1, 2, 26, 51](#) 

External link

Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:



- “a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Article 5(2) requires that:



“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

Further Reading

 [Relevant provisions in the GDPR - see Article 5 and Recital 39](#) 

External link

Lawful basis for processing

At a glance

- You must have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

Checklist

- We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity.
- We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.
- We have documented our decision on which lawful basis applies to help us demonstrate compliance.
- We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.
- Where we process special category data, we have also identified a condition for processing special category data, and have documented this.
- Where we process criminal offence data, we have also identified a condition for processing this data, and have documented this.

In brief

- [What's new?](#)
- [Why is the lawful basis for processing important?](#)
- [What are the lawful bases?](#)
- [When is processing 'necessary'?](#)
- [How do we decide which lawful basis applies?](#)
- [When should we decide on our lawful basis?](#)
- [What happens if we have a new purpose?](#)
- [How should we document our lawful basis?](#)
- [What do we need to tell people?](#)
- [What about special category data?](#)
- [What about criminal conviction data?](#)

What's new?

The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act 1998 (the 1998 Act). However, the GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing.

The six lawful bases for processing are broadly similar to the old conditions for processing, although there are some differences. You now need to review your existing processing, identify the most appropriate lawful basis, and check that it applies. In many cases it is likely to be the same as your existing condition for processing.

The biggest change is for public authorities, who now need to consider the new 'public task' basis first for most of their processing, and have more limited scope to rely on consent or legitimate interests.

You can choose a new lawful basis if you find that your old condition for processing is no longer appropriate under the GDPR, or decide that a different basis is more appropriate. You should try to get this right first time. Once the GDPR is in effect, it will be much harder to swap between lawful bases as will if you find that your original basis was invalid. You will be in breach of the GDPR if you did not clearly identify the appropriate lawful basis (or bases, if more than one applies) from the start.

The GDPR brings in new accountability and transparency requirements. You should therefore make sure you clearly document your lawful basis so that you can demonstrate your compliance in line with Articles 5(2) and 24.

You must now inform people upfront about your lawful basis for processing their personal data. You need therefore to communicate this information to individuals by 25 May 2018, and ensure that you include it in all future privacy notices.

Further Reading

 [Relevant provisions in the GDPR - See Article 6 and Recital 171, and Article 5\(2\)](#) 

External link

Why is the lawful basis for processing important?

The first principle requires that you process all personal data lawfully, fairly and in a transparent manner. Processing is only lawful if you have a lawful basis under Article 6. And to comply with the accountability principle in Article 5(2), you must be able to demonstrate that a lawful basis applies.

If no lawful basis applies to your processing, your processing will be unlawful and in breach of the first principle. Individuals also have the right to erase personal data which has been processed unlawfully.

The individual's right to be informed under Article 13 and 14 requires you to provide people with information about your lawful basis for processing. This means you need to include these details in your privacy notice.

The lawful basis for your processing can also affect which rights are available to individuals. For example, some rights will not apply:

	Right to erasure	Right to portability	Right to object
Consent			✘ but right to withdraw consent
Contract			✘
Legal obligation	✘	✘	✘
Vital interests		✘	✘
Public task	✘	✘	
Legitimate interests		✘	

However, an individual always has the right to object to processing for the purposes of direct marketing, whatever lawful basis applies.

The remaining rights are not always absolute, and there are other rights which may be affected in other ways. For example, your lawful basis may affect how provisions relating to automated decisions and profiling apply, and if you are relying on legitimate interests you need more detail in your privacy notice to comply with the right to be informed.

Please read the section of this Guide on individuals' rights for full details.

Further Reading

 [Relevant provisions in the GDPR - See Article 6 and Recitals 39, 40, and Chapter III \(Rights of the data subject\)](#) 

External link

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For more detail on each lawful basis, read the relevant page of this guide.

Further Reading

 [Relevant provisions in the GDPR - See Article 6\(1\), Article 6\(2\) and Recital 40](#) 

External link

When is processing 'necessary'?

Many of the lawful bases for processing depend on the processing being "necessary". This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is a necessary for the stated purpose, not whether it is a necessary part of your chosen method of pursuing that purpose.

How do we decide which lawful basis applies?

This depends on your specific purposes and the context of the processing. You should consider which lawful basis best fits the circumstances. You might consider that more than one basis applies, in which case you should identify and document all of them from the start.

You must not adopt a one-size-fits-all approach. No one basis should be seen as always better, safer or more important than the others, and there is no hierarchy in the order of the list in the GDPR.

You may need to consider a variety of factors, including:

- What is your purpose – what are you trying to achieve?
- Can you reasonably achieve it in a different way?
- Do you have a choice over whether or not to process the data?
- Are you a public authority?

Several of the lawful bases relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to

consider these first.

If you are a public authority and can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the individual. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the GDPR does restrict public authorities' use of these two bases.

The Data Protection Bill will define 'public authority' and the final text of those provisions may also have some impact here. We will publish more guidance on the effect of relevant Bill provisions when they are finalised.

Example

A university that wants to process personal data may consider a variety of lawful bases depending on what it wants to do with the data.

Universities are likely to be classified as public authorities, so the public task basis is likely to apply to much of their processing, depending on the detail of their constitutions and legal powers. If the processing is separate from their tasks as a public authority, then the university may instead wish to consider whether consent or legitimate interests are appropriate in the particular circumstances, considering the factors set out below. For example, a University might rely on public task for processing personal data for teaching and research purposes; but a mixture of legitimate interests and consent for alumni relations and fundraising purposes.

The university however needs to consider its basis carefully – it is the controller's responsibility to be able to demonstrate which lawful basis applies to the particular processing purpose.

If you are processing for purposes other than legal obligation, contract, vital interests or public task, then the appropriate lawful basis may not be so clear cut. In many cases you are likely to have a choice between using legitimate interests or consent. You need to give some thought to the wider context, including:

- Who does the processing benefit?
- Would individuals expect this processing to take place?
- What is your relationship with the individual?
- Are you in a position of power over them?
- What is the impact of the processing on the individual?
- Are they vulnerable?
- Are some of the individuals concerned likely to object?
- Are you able to stop the processing at any time on request?

You may prefer to consider legitimate interests as your lawful basis if you wish to keep control over the processing and take responsibility for demonstrating that it is in line with people's reasonable expectations and wouldn't have an unwarranted impact on them. On the other hand, if you prefer to give individuals full control over and responsibility for their data (including the ability to change their

mind as to whether it can continue to be processed), you may want to consider relying on individuals' consent.

When should we decide on our lawful basis?

You must determine your lawful basis before starting to process personal data. It's important to get this right first time. If you find at a later date that your chosen basis was actually inappropriate, it will be difficult to simply swap to a different one. Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements.

Example

A company decided to process on the basis of consent, and obtained consent from individuals. An individual subsequently decided to withdraw their consent to the processing of their data, as is their right. However, the company wanted to keep processing the data so decided to continue the processing on the basis of legitimate interests.

Even if it could have originally relied on legitimate interests, the company cannot do so at a later date – it cannot switch basis when it realised that the original chosen basis was inappropriate (in this case, because it did not want to offer the individual genuine ongoing control). It should have made clear to the individual from the start that it was processing on the basis of legitimate interests. Leading the individual to believe they had a choice is inherently unfair if that choice will be irrelevant. The company must therefore stop processing when the individual withdraws consent.

It is therefore important to thoroughly assess upfront which basis is appropriate and document this. It may be possible that more than one basis applies to the processing because you have more than one purpose, and if this is the case then you should make this clear from the start.

If there is a genuine change in circumstances or you have a new and unanticipated purpose which means there is a good reason to review your lawful basis and make a change, you need to inform the individual and document the change.

Further Reading

 [Relevant provisions in the GDPR - See Article 6\(1\) and Recitals 39 and 40](#) 

External link

What happens if we have a new purpose?

If your purposes change over time or you have a new purpose which you did not originally anticipate, you may not need a new lawful basis as long as your new purpose is compatible with the original purpose.

However, the GDPR specifically says this does not apply to processing based on consent. Consent must always be specific and informed. You need to either get fresh consent which specifically covers the new

purpose, or find a different basis for the new purpose. If you do get specific consent for the new purpose, you do not need to show it is compatible.

In other cases, in order to assess whether the new purpose is compatible with the original purpose you should take into account:

- any link between your initial purpose and the new purpose;
- the context in which you collected the data – in particular, your relationship with the individual and what they would reasonably expect;
- the nature of the personal data – eg is it special category data or criminal offence data;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards - eg encryption or pseudonymisation.

This list is not exhaustive and what you need to look at depends on the particular circumstances.

As a general rule, if the new purpose is very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is unlikely to be compatible with your original purpose for collecting the data. You need to identify and document a new lawful basis to process the data for that new purpose.

The GDPR specifically says that further processing for the following purposes should be considered to be compatible lawful processing operations:

- archiving purposes in the public interest;
- scientific research purposes; and
- statistical purposes.

There is a link here to the 'purpose limitation' principle in Article 5, which states that "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".

Even if the processing for a new purpose is lawful, you will also need to consider whether it is fair and transparent, and give individuals information about the new purpose.

Further Reading

 [Relevant provisions in the GDPR - See Article 6\(4\), Article 5\(1\)\(b\) and Recital 50, Recital 61](#) 

External link

How should we document our lawful basis?

The principle of accountability requires you to be able to demonstrate that you are complying with the GDPR, and have appropriate policies and processes. This means that you need to be able to show that you have properly considered which lawful basis applies to each processing purpose and can justify your decision.

You need therefore to keep a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies. There is no standard form for this, as long as you ensure that what you record is sufficient to demonstrate that a lawful basis applies. This will help you comply

with accountability obligations, and will also help you when writing your privacy notices.

It is your responsibility to ensure that you can demonstrate which lawful basis applies to the particular processing purpose.

Read the accountability section of this guide for more on this topic. There is also further guidance on documenting consent or legitimate interests assessments in the relevant pages of the guide.

Further Reading

 [Relevant provisions in the GDPR - See Articles 5\(2\) and 24](#) 
External link

What do we need to tell people?

You need to include information about your lawful basis (or bases, if more than one applies) in your privacy notice. Under the transparency provisions of the GDPR, the information you need to give people includes:

- your intended purposes for processing the personal data; and
- the lawful basis for the processing.

This applies whether you collect the personal data directly from the individual or you collect their data from another source.

Read the 'right to be informed' section of this guide for more on the transparency requirements of the GDPR.

Further Reading

 [Relevant provisions in the GDPR - See Article 13\(1\)\(c\), Article 14\(1\)\(c\) and Recital 39](#) 
External link

What about special category data?

If you are processing special category data, you need to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability.

Further guidance can be found in the section on [special category data](#).

What about criminal offence data?

If you are processing data about criminal convictions, criminal offences or related security measures,

you need both a lawful basis for processing and a separate condition for processing this data in compliance with Article 10. You should document both your lawful basis for processing and your criminal offence data condition so that you can demonstrate compliance and accountability.

Further guidance can be found in the section on [criminal offence data](#).

In more detail – ICO guidance

We have produced the [lawful basis interactive guidance tool](#), to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

Consent

At a glance

- The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.
- Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.
- Check your consent practices and your existing consents. Refresh your consents if they don't meet the GDPR standard.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent to processing a precondition of a service.
- Public authorities and employers will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent.

Checklists

Asking for consent

- We have checked that consent is the most appropriate lawful basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don't use pre-ticked boxes or any other type of default consent.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.
- We give separate distinct ('granular') options to consent separately to different purposes and

types of processing.

- We name our organisation and any third party controllers who will be relying on the consent.
- We tell individuals they can withdraw their consent.
- We ensure that individuals can refuse to consent without detriment.
- We avoid making consent a precondition of a service.
- If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording consent

- We keep a record of when and how we got consent from the individual.
- We keep a record of exactly what they were told at the time.

Managing consent

- We regularly review consents to check that the relationship, the processing and the purposes have not changed.
- We have processes in place to refresh consent at appropriate intervals, including any parental consents.
- We consider using privacy dashboards or other preference-management tools as a matter of good practice.
- We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.
- We act on withdrawals of consent as soon as we can.
- We don't penalise individuals who wish to withdraw consent.

In brief

- [What's new?](#)
- [Why is consent important?](#)
- [When is consent appropriate?](#)

- [What is valid consent?](#)
- [How should we obtain, record and manage consent?](#)

What's new?

The GDPR sets a high standard for consent, but the biggest change is what this means in practice for your consent mechanisms.

The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

You must keep clear records to demonstrate consent.

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent.

You need to review existing consents and your consent mechanisms to check they meet the GDPR standard. If they do, there is no need to obtain fresh consent.

Why is consent important?

Consent is one lawful basis for processing, and explicit consent can also legitimise use of special category data. Consent may also be relevant where the individual has exercised their right to restriction, and explicit consent can legitimise automated decision-making and overseas transfers of data.

Genuine consent should put individuals in control, build trust and engagement, and enhance your reputation.

Relying on inappropriate or invalid consent could destroy trust and harm your reputation – and may leave you open to large fines.

When is consent appropriate?

Consent is one lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, you should consider using an alternative.

Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.

If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis.

Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.

What is valid consent?

Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their data.

Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.

Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity.

Explicit consent must be expressly confirmed in words, rather than by any other positive action.

There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

How should we obtain, record and manage consent?

Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand. Include:

- the name of your organisation;
- the name of any third party controllers who will rely on the consent;
- why you want the data;
- what you will do with it; and
- that individuals can withdraw consent at any time.

You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or other default settings. Wherever possible, give separate ('granular') options to consent to different purposes and different types of processing.

Keep records to evidence consent – who consented, when, how, and what they were told.

Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.

Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

Further Reading

 [Relevant provisions in the GDPR - See Articles 4\(11\), 6\(1\)\(a\) 7, 8, 9\(2\)\(a\) and Recitals 32, 38, 40, 42, 43, 171](#) 

External link

In more detail - ICO guidance

We have produced more detailed guidance on [consent](#).

We have produced [an interactive guidance tool](#) to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

In more detail - Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 adopted [Guidelines on consent](#)  on 10 April 2018.

Contract

At a glance

- You can rely on this lawful basis if you need to process someone's personal data:
 - to fulfil your contractual obligations to them; or
 - because they have asked you to do something before entering into a contract (eg provide a quote).
- The processing must be necessary. If you could reasonably do what they want without processing their personal data, this basis will not apply.
- You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.

In brief

- [What's new?](#)
- [What does the GDPR say?](#)
- [When is the lawful basis for contracts likely to apply?](#)
- [When is processing 'necessary' for a contract?](#)
- [What else should we consider?](#)

What's new?

Very little. The lawful basis for processing necessary for contracts is almost identical to the old condition for processing in paragraph 2 of Schedule 2 of the 1998 Act.

You need to review your existing processing so that you can document where you rely on this basis and inform individuals. But in practice, if you are confident that your existing approach complied with the 1998 Act, you are unlikely to need to change your existing basis for processing.

What does the GDPR say?

Article 6(1)(b) gives you a lawful basis for processing where:



“processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”

When is the lawful basis for contracts likely to apply?

You have a lawful basis for processing if:

- you have a contract with the individual and you need to process their personal data to comply with your obligations under the contract.
- you haven't yet got a contract with the individual, but they have asked you to do something as a first step (eg provide a quote) and you need to process their personal data to do what they ask.

It does not apply if you need to process one person's details but the contract is with someone else.

It does not apply if you take pre-contractual steps on your own initiative or at the request of a third party.

Example

An individual shopping around for car insurance requests a quotation. The insurer needs to process certain data in order to prepare the quotation, such as the make and age of the car.

Note that, in this context, a contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, you both intend them to be legally binding, and there is an element of exchange (usually an exchange of goods or services for money, but this can be anything of value). However, this is not a full explanation of contract law, and if in doubt you should seek your own legal advice.

When is processing 'necessary' for a contract?

'Necessary' does not mean that the processing must be essential for the purposes of performing a contract or taking relevant pre-contractual steps. However, it must be a targeted and proportionate way of achieving that purpose. This lawful basis does not apply if there are other reasonable and less intrusive ways to meet your contractual obligations or take the steps requested.

The processing must be necessary to deliver your side of the contract with this particular person. If the processing is only necessary to maintain your business model more generally, this lawful basis will not apply and you should consider another lawful basis, such as legitimate interests.

Example

When a data subject makes an online purchase, a controller processes the address of the individual in order to deliver the goods. This is necessary in order to perform the contract.

However, the profiling of an individual's interests and preferences based on items purchased is not necessary for the performance of the contract and the controller cannot rely on Article 6(1)(b) as the lawful basis for this processing. Even if this type of targeted advertising is a useful part of your customer relationship and is a necessary part of your business model, it is not necessary to perform the contract itself.

This does not mean that processing which is not necessary for the contract is automatically unlawful, but rather that you need to look for a different lawful basis.

What else should we consider?

If the processing is necessary for a contract with the individual, processing is lawful on this basis and you do not need to get separate consent.

If processing of special category data is necessary for the contract, you also need to identify a separate condition for processing this data. Read our guidance on special category data for more information.

If the contract is with a child under 18, you need to consider whether they have the necessary competence to enter into a contract. If you have doubts about their competence, you may wish to consider an alternative basis such as legitimate interests, which can help you to demonstrate that the child's rights and interests are properly considered and protected. Read our guidance on children and the GDPR for more information.

If the processing is not necessary for the contract, you need to consider another lawful basis such as legitimate interests or consent. Note that if you want to rely on consent you will not generally be able to make the processing a condition of the contract. Read our guidance on consent for more information.

If you are processing on the basis of contract, the individual's right to object and right not to be subject to a decision based solely on automated processing will not apply. However, the individual will have a right to data portability. Read our guidance on individual rights for more information.

Remember to document your decision that processing is necessary for the contract, and include information about your purposes and lawful basis in your privacy notice.

Further Reading

 [Relevant provisions in the GDPR - See Article 6\(1\)\(b\) and Recital 44](#) 

External link

In more detail - ICO guidance

We have produced the [lawful basis interactive guidance tool](#), to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

Legal obligation

At a glance

- You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation.
- This does not apply to contractual obligations.
- The processing must be necessary. If you can reasonably comply without processing the personal data, this basis does not apply.
- You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.
- You should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your obligation.

In brief

- [What's new?](#)
- [What does the GDPR say?](#)
- [When is the lawful basis for legal obligations likely to apply?](#)
- [When is processing 'necessary' for compliance?](#)
- [What else should we consider?](#)

What's new?

Very little. The lawful basis for processing necessary for compliance with a legal obligation is almost identical to the old condition for processing in paragraph 3 of Schedule 2 of the 1998 Act.

You need to review your existing processing so that you can document where you rely on this basis and inform individuals. But in practice, if you are confident that your existing approach complied with the 1998 Act, you are unlikely to need to change your existing basis for processing.

What does the GDPR say?

Article 6(1)(c) provides a lawful basis for processing where:



“processing is necessary for compliance with a legal obligation to which the controller is subject.”

When is the lawful basis for legal obligations likely to apply?

In short, when you are obliged to process the personal data to comply with the law.

Article 6(3) requires that the legal obligation must be laid down by UK or EU law. Recital 41 confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. So it includes clear common law obligations.

This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

You should be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you can refer to a government website or to industry guidance that explains generally applicable legal obligations.

Example

An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to HMRC.

The employer can point to the HMRC website where the requirements are set out to demonstrate this obligation. In this situation it is not necessary to cite each specific piece of legislation.

Example

A financial institution relies on the legal obligation imposed by the Part 7 of Proceeds of Crime Act 2002 to process personal data in order submit a Suspicious Activity Report to the National Crime Agency when it knows or suspects that a person is engaged in, or attempting, money laundering.

Example

A court order may require you to process personal data for a particular purpose and this also qualifies as a legal obligation.

Regulatory requirements also qualify as a legal obligation for these purposes where there is a statutory basis underpinning the regulatory regime and which requires regulated organisations to comply.

Example

The Competition and Markets Authority (CMA) has powers under The Enterprise Act 2002 to make orders to remedy adverse effects on competition, some of which may require the processing of personal data.

A retail energy supplier passes customer data to the Gas and Electricity Markets Authority to comply with the CMA's Energy Market Investigation (Database) Order 2016. The supplier may rely on legal obligation as the lawful basis for this processing.

A contractual obligation does not comprise a legal obligation in this context. You cannot contract out of the requirement for a lawful basis. However, you can look for a different lawful basis. If the contract is with the individual you can consider the lawful basis for contracts. For contracts with other parties, you may want to consider legitimate interests.

When is processing 'necessary' for compliance?

Although the processing need not be essential for you to comply with the legal obligation, it must be a reasonable and proportionate way of achieving compliance. You cannot rely on this lawful basis if you have discretion over whether to process the personal data, or if there is another reasonable way to comply.

It is likely to be clear from the law in question whether the processing is actually necessary for compliance.

What else should we consider?

If you are processing on the basis of legal obligation, the individual has no right to erasure, right to data portability, or right to object. Read our guidance on individual rights for more information.

Remember to:

- document your decision that processing is necessary for compliance with a legal obligation;
- identify an appropriate source for the obligation in question; and
- include information about your purposes and lawful basis in your privacy notice.

Further Reading

 [Relevant provisions in the GDPR - See Article 6\(1\)\(c\), Recitals 41, 45](#) 
External link

In more detail - ICO guidance

We have produced the [lawful basis interactive guidance tool](#), to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

Vital interests

At a glance

- You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.
- The processing must be necessary. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.
- You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.
- You should consider whether you are likely to rely on this basis, and if so document the circumstances where it will be relevant and ensure you can justify your reasoning.

In brief

- [What's new?](#)
- [What does the GDPR say?](#)
- [What are 'vital interests'?](#)
- [When is the vital interests basis likely to apply?](#)
- [What else should we consider?](#)

What's new?

The lawful basis for vital interests is very similar to the old condition for processing in paragraph 4 of Schedule 2 of the 1998 Act. One key difference is that anyone's vital interests can now provide a basis for processing, not just those of the data subject themselves.

You need to review your existing processing to identify if you have any ongoing processing for this reason, or are likely to need to process for this reason in future. You should then document where you rely on this basis and inform individuals if relevant.

What does the GDPR say?

Article 6(1)(d) provides a lawful basis for processing where:



"processing is necessary in order to protect the vital interests of the data subject or of another natural person".

Recital 46 provides some further guidance:



“The processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis...”

What are ‘vital interests’?

It’s clear from Recital 46 that vital interests are intended to cover only interests that are essential for someone’s life. So this lawful basis is very limited in its scope, and generally only applies to matters of life and death.

When is the vital interests basis likely to apply?

It is likely to be particularly relevant for emergency medical care, when you need to process personal data for medical purposes but the individual is incapable of giving consent to the processing.

Example

An individual is admitted to the A & E department of a hospital with life-threatening injuries following a serious road accident. The disclosure to the hospital of the individual’s medical history is necessary in order to protect his/her vital interests.

It is less likely to be appropriate for medical care that is planned in advance. Another lawful basis such as public task or legitimate interests is likely to be more appropriate in this case.

Processing of one individual’s personal data to protect the vital interests of others is likely to happen more rarely. It may be relevant, for example, if it is necessary to process a parent’s personal data to protect the vital interests of a child.

Vital interests is also less likely to be the appropriate basis for processing on a larger scale. Recital 46 does suggest that vital interests might apply where you are processing on humanitarian grounds such as monitoring epidemics, or where there is a natural or man-made disaster causing a humanitarian emergency.

However, if you are processing one person’s personal data to protect someone else’s life, Recital 46 also indicates that you should generally try to use an alternative lawful basis, unless none is obviously available. For example, in many cases you could consider legitimate interests, which will give you a framework to balance the rights and interests of the data subject(s) with the vital interests of the person or people you are trying to protect.

What else should we consider?

In most cases the protection of vital interests is likely to arise in the context of health data. This is one of the special categories of data, which means you will also need to identify a condition for processing special category data under Article 9.

There is a specific condition at Article 9(2)(c) for processing special category data where necessary to protect someone's vital interests. However, this only applies if the data subject is physically or legally incapable of giving consent. This means explicit consent is more appropriate in many cases, and you cannot in practice rely on vital interests for special category data (including health data) if the data subject refuses consent, unless they are not competent to do so.

Further Reading

 [Relevant provisions in the GDPR - See Article 6\(1\)\(d\), Article 9\(2\)\(c\), Recital 46](#) 

External link

In more detail - ICO guidance

We have produced the [lawful basis interactive guidance tool](#), to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

Public task

At a glance

- You can rely on this lawful basis if you need to process personal data:
 - 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or
 - to perform a specific task in the public interest that is set out in law.
- It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.
- You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law.
- The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.
- Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis.

In brief

- [What's new under the GDPR?](#)
- [What is the 'public task' basis?](#)
- [What does 'laid down by law' mean?](#)
- [Who can rely on this basis?](#)
- [When can we rely on this basis?](#)
- [What else should we consider?](#)

What's new under the GDPR?

The public task basis in Article 6(1)(e) may appear new, but it is similar to the old condition for processing for functions of a public nature in Schedule 2 of the Data Protection Act 1998.

One key difference is that the GDPR says that the relevant task or function must have a clear basis in law.

The GDPR is also clear that public authorities can no longer rely on legitimate interests for processing carried out in performance of their tasks. In the past, some of this type of processing may have been done on the basis of legitimate interests. If you are a public authority, this means you may now need to consider the public task basis for more of your processing.

The GDPR also brings in new accountability requirements. You should document your lawful basis so that you can demonstrate that it applies. In particular, you should be able to identify a clear basis in either statute or common law for the relevant task, function or power for which you are using the personal

data.

You must also update your privacy notice to include your lawful basis, and communicate this to individuals.

What is the ‘public task’ basis?

Article 6(1)(e) gives you a lawful basis for processing where:



“processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”

This can apply if you are either:

- carrying out a specific task in the public interest which is laid down by law; or
- exercising official authority (for example, a public body’s tasks, functions, duties or powers) which is laid down by law.

If you can show you are exercising official authority, including use of discretionary powers, there is no additional public interest test. However, you must be able to demonstrate that the processing is ‘necessary’ for that purpose.

‘Necessary’ means that the processing must be a targeted and proportionate way of achieving your purpose. You do not have a lawful basis for processing if there is another reasonable and less intrusive way to achieve the same result.

In this guide we use the term ‘public task’ to help describe and label this lawful basis. However, this is not a term used in the GDPR itself. Your focus should be on demonstrating either that you are carrying out a task in the public interest, or that you are exercising official authority.

In particular, there is no direct link to the concept of ‘public task’ in the Re-use of Public Sector Information Regulations 2015 (RPSI). There is some overlap, as a public sector body’s core role and functions for RPSI purposes may be a useful starting point in demonstrating official authority for these purposes. However, you shouldn’t assume that it is an identical test. See our [Guide to RPSI](#) for more on public task in the context of RPSI.

What does ‘laid down by law’ mean?

Article 6(3) requires that the relevant task or authority must be laid down by domestic or EU law. This will most often be a statutory function. However, Recital 41 clarifies that this does not have to be an explicit statutory provision, as long as the application of the law is clear and foreseeable. This means that it includes clear common law tasks, functions or powers as well as those set out in statute or statutory guidance.

You do not need specific legal authority for the particular processing activity. The point is that your overall purpose must be to perform a public interest task or exercise official authority, and that overall

task or authority has a sufficiently clear basis in law.

Who can rely on this basis?

Any organisation who is exercising official authority or carrying out a specific task in the public interest. The focus is on the nature of the function, not the nature of the organisation.

Example

Private water companies are likely to be able to rely on the public task basis even if they do not fall within the definition of a public authority in the Data Protection Bill. This is because they are considered to be carrying out functions of public administration and they exercise special legal powers to carry out utility services in the public interest. See our guidance on [Public authorities under the EIR](#) for more details.

However, if you are a private sector organisation you are likely to be able to consider the legitimate interests basis as an alternative.

See the main lawful basis page of this guide for more on how to choose the most appropriate basis.

When can we rely on this basis?

The Data Protection Bill includes a draft clause clarifying that the public task basis will cover processing necessary for:

- the administration of justice;
- parliamentary functions;
- statutory functions; or
- governmental functions.

However, this is not intended as an exhaustive list. If you have other official non-statutory functions or public interest tasks you can still rely on the public task basis, as long as the underlying legal basis for that function or task is clear and foreseeable.

For accountability purposes, you should be able to specify the relevant task, function or power, and identify its basis in common law or statute. You should also ensure that you can demonstrate there is no other reasonable and less intrusive means to achieve your purpose.

What else should we consider?

Individuals' rights to erasure and data portability do not apply if you are processing on the basis of public task. However, individuals do have a right to object. See our guidance on individual rights for more information.

You should consider an alternative lawful basis if you are not confident that processing is necessary for a relevant task, function or power which is clearly set out in law.

If you are a public authority (as defined in the Data Protection Bill), your ability to rely on consent or legitimate interests as an alternative basis is more limited, but they may be available in some circumstances. In particular, legitimate interests is still available for processing which falls outside your tasks as a public authority. Other lawful bases may also be relevant. See our guidance on the other lawful bases for more information. We will publish more guidance on the definition of a public authority when the relevant Bill provisions are finalised.

Remember that the GDPR specifically says that further processing for certain purposes should be considered to be compatible with your original purpose. This means that if you originally processed the personal data for a relevant task or function, you do not need a separate lawful basis for any further processing for:

- archiving purposes in the public interest;
- scientific research purposes; or
- statistical purposes.

If you are processing special category data, you also need to identify an additional condition for processing this type of data. Read our guidance on special category data for more information. The Data Protection Bill includes specific draft conditions for parliamentary, statutory or governmental functions in the substantial public interest – more guidance on this and other conditions will follow when the Bill is finalised.

To help you meet your accountability and transparency obligations, remember to:

- document your decision that the processing is necessary for you to perform a task in the public interest or exercise your official authority;
- identify the relevant task or authority and its basis in common law or statute; and
- include basic information about your purposes and lawful basis in your privacy notice.

Further Reading

 [Relevant provisions in the GDPR - See Article 6\(1\)\(e\) and 6\(3\), and Recitals 41, 45 and 50](#) 
External link

 [Relevant provisions in the Data Protection Bill - See clause 8 and Schedule 1 para 6 and 7](#) 
External link

In more detail – ICO guidance

We are planning to develop more detailed guidance on this topic.

We have produced the [lawful basis interactive guidance tool](#), to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

Legitimate interests

At a glance

- Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.
- It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
- Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.
- There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:
 - identify a legitimate interest;
 - show that the processing is necessary to achieve it; and
 - balance it against the individual's interests, rights and freedoms.
- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy information.

Checklists

- We have checked that legitimate interests is the most appropriate basis.
- We understand our responsibility to protect the individual's interests.
- We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.
- We have identified the relevant legitimate interests.
- We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

- We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.
- We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.
- We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
- If we process children's data, we take extra care to make sure we protect their interests.
- We have considered safeguards to reduce the impact where possible.
- We have considered whether we can offer an opt out.
- If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.
- We keep our LIA under review, and repeat it if circumstances change.
- We include information about our legitimate interests in our privacy information.

In brief

- [What's new under the GDPR?](#)
- [What is the 'legitimate interests' basis?](#)
- [When can we rely on legitimate interests?](#)
- [How can we apply legitimate interests in practice?](#)
- [What else do we need to consider?](#)

What's new under the GDPR?

The concept of legitimate interests as a lawful basis for processing is essentially the same as the equivalent Schedule 2 condition in the 1998 Act, with some changes in detail.

You can now consider the legitimate interests of any third party, including wider benefits to society. And when weighing against the individual's interests, the focus is wider than the emphasis on 'unwarranted prejudice' to the individual in the 1998 Act. For example, unexpected processing is likely to affect whether the individual's interests override your legitimate interests, even without specific harm.

The GDPR is clearer that you must give particular weight to protecting children's data.

Public authorities are more limited in their ability to rely on legitimate interests, and should consider the 'public task' basis instead for any processing they do to perform their tasks as a public authority. Legitimate interests may still be available for other legitimate processing outside of those tasks.

The biggest change is that you need to document your decisions on legitimate interests so that you can demonstrate compliance under the new GDPR accountability principle. You must also include more information in your privacy information.

In the run up to 25 May 2018, you need to review your existing processing to identify your lawful basis and document where you rely on legitimate interests, update your privacy information, and communicate it to individuals.

What is the 'legitimate interests' basis?

Article 6(1)(f) gives you a lawful basis for processing where:



“processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

This can be broken down into a three-part test:

1. **Purpose test:** are you pursuing a legitimate interest?
2. **Necessity test:** is the processing necessary for that purpose?
3. **Balancing test:** do the individual's interests override the legitimate interest?

A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test.

The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. It also says that you have a legitimate interest in disclosing information about possible criminal acts or security threats to the authorities.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result.

You must balance your interests against the individual's interests. In particular, if they would not reasonably expect you to use data in that way, or it would cause them unwarranted harm, their interests are likely to override yours. However, your interests do not always have to align with the individual's interests. If there is a conflict, your interests can still prevail as long as there is a clear justification for the impact on the individual.

When can we rely on legitimate interests?

Legitimate interests is the most flexible lawful basis, but you cannot assume it will always be appropriate for all of your processing.

If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected.

Legitimate interests is most likely to be an appropriate basis where you use data in ways that people

would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified.

You can rely on legitimate interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object – but only if you don't need consent under PECR. See our [Guide to PECR](#) for more on when you need consent for electronic marketing.

You can consider legitimate interests for processing children's data, but you must take extra care to make sure their interests are protected. See our detailed guidance on [children and the GDPR](#).

You may be able to rely on legitimate interests in order to lawfully disclose personal data to a third party. You should consider why they want the information, whether they actually need it, and what they will do with it. You need to demonstrate that the disclosure is justified, but it will be their responsibility to determine their lawful basis for their own processing.

You should avoid using legitimate interests if you are using personal data in ways people do not understand and would not reasonably expect, or if you think some people would object if you explained it to them. You should also avoid this basis for processing that could cause harm, unless you are confident there is nevertheless a compelling reason to go ahead which justifies the impact.

If you are a public authority, you cannot rely on legitimate interests for any processing you do to perform your tasks as a public authority. However, if you have other legitimate purposes outside the scope of your tasks as a public authority, you can consider legitimate interests where appropriate. This will be particularly relevant for public authorities with commercial interests.

See our guidance page on the lawful basis for more information on the alternatives to legitimate interests, and how to decide which basis to choose.

How can we apply legitimate interests in practice?

If you want to rely on legitimate interests, you can use the three-part test to assess whether it applies. We refer to this as a legitimate interests assessment (LIA) and you should do it before you start the processing.

An LIA is a type of light-touch risk assessment based on the specific context and circumstances. It will help you ensure that your processing is lawful. Recording your LIA will also help you demonstrate compliance in line with your accountability obligations under Articles 5(2) and 24. In some cases an LIA will be quite short, but in others there will be more to consider.

First, identify the legitimate interest(s). Consider:

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

Second, apply the necessity test. Consider:

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Third, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are you processing children's data?
- Are any of the individuals vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

You then need to make a decision about whether you still think legitimate interests is an appropriate basis. There's no foolproof formula for the outcome of the balancing test – but you must be confident that your legitimate interests are not overridden by the risks you have identified.

Keep a record of your LIA and the outcome. There is no standard format for this, but it's important to record your thinking to help show you have proper decision-making processes in place and to justify the outcome.

Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing.

If you are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis. Legitimate interests will not often be the most appropriate basis for processing which is unexpected or high risk.

If your LIA identifies significant risks, consider whether you need to do a DPIA to assess the risk and potential mitigation in more detail. See our guidance on DPIAs for more on this.

What else do we need to consider?

You must tell people in your privacy information that you are relying on legitimate interests, and explain what these interests are.

If you want to process the personal data for a new purpose, you may be able to continue processing under legitimate interests as long as your new purpose is compatible with your original purpose. We would still recommend that you conduct a new LIA, as this will help you demonstrate compatibility.

If you rely on legitimate interests, the right to data portability does not apply.

If you are relying on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects. For other purposes, you must stop unless you can show that your legitimate interests are compelling enough to override the individual's rights. See our guidance on individual rights for more on this.

Further Reading

 [Relevant provisions in the GDPR - See Article 6\(1\)\(f\) and Recitals 47, 48 and 49](#) 
External link

In more detail – ICO guidance

We have produced more detailed guidance on [legitimate interests](#)

We have produced the [lawful basis interactive guidance tool](#), to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

In more detail - Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

There are no immediate plans for Article 29 Working Party guidance on legitimate interests under the GDPR, but [WP29 Opinion 06/2014 \(9 April 2014\)](#) gives detailed guidance on the key elements of the similar legitimate interests provisions under the previous Data Protection Directive 95/46/EC.

Special category data

At a glance

- Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.
- In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.
- There are ten conditions for processing special category data in the GDPR itself, but the Data Protection Bill will introduce additional conditions and safeguards.
- You must determine your condition for processing special category data before you begin this processing under the GDPR, and you should document it.

In brief

- [What's new?](#)
- [What's different about special category data?](#)
- [What are the conditions for processing special category data?](#)

What's new?

Special category data is broadly similar to the concept of sensitive personal data under the 1998 Act. The requirement to identify a specific condition for processing this type of data is also very similar.

One change is that the GDPR includes genetic data and some biometric data in the definition. Another is that it does not include personal data relating to criminal offences and convictions, as there are separate and specific safeguards for this type of data in Article 10. See the definitions section of this Guide for more detail on what counts as special category data.

The conditions for processing special category data under the GDPR in the UK are likely to be similar to the Schedule 3 conditions under the 1998 Act for the processing of sensitive personal data. More detailed guidance on the special category conditions and how they differ from existing Schedule 3 conditions will follow as the Data Protection Bill is finalised.

What's different about special category data?

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that you will also need to satisfy a specific condition under Article 9.

This is because special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- race;

- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

See the definitions section of this Guide for full details.

In particular, this type of data could create more significant risks to a person’s fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Your choice of lawful basis under Article 6 does not dictate which special category condition you must apply, and vice versa. For example, if you use consent as your lawful basis, you are not restricted to using explicit consent for special category processing under Article 9. You should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two. For example, if your lawful basis is vital interests, it is highly likely that the Article 9 condition for vital interests will also be appropriate.

What are the conditions for processing special category data?

The conditions are listed in Article 9(2) of the GDPR:



- (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

- (e) processing relates to personal data which are manifestly made public by the data subject;
- (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Some of these conditions make reference to UK law, and the GDPR also gives member states the scope to add more conditions. The Data Protection Bill includes proposals for additional conditions and safeguards, and we will publish more detailed guidance here once these provisions are finalised.

Further Reading

 [Relevant provisions in the GDPR - See Article 9\(2\) and Recital 51](#) 

External link

 [Relevant provisions in the Data Protection Bill - See clauses 9 and 10, and Schedule 1](#) 

External link

Criminal offence data

At a glance

- To process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.
- The Data Protection Bill deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.
- You can also process this type of data if you have official authority to do so because you are processing the data in an official capacity.
- You cannot keep a comprehensive register of criminal convictions unless you do so in an official capacity.
- You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this.

In brief

- [What's new?](#)
- [What is criminal offence data?](#)
- [What's different about criminal offence data?](#)
- [What are the conditions for processing criminal offence data?](#)

What's new?

The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10.

Article 10 also specifies that you can only keep a comprehensive register of criminal convictions if you are doing so under the control of official authority.

What is criminal offence data?

Article 10 applies to personal data relating to criminal convictions and offences, or related security measures. In this guidance, we refer to this as criminal offence data.

This concept of criminal offence data includes the type of data about criminal allegations, proceedings or convictions that would have been sensitive personal data under the 1998 Act. However, it is potentially broader than this. In particular, Article 10 specifically extends to personal data linked to related security measures.

What's different about criminal offence data?

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that if you are processing personal criminal offence data, you will

also need to comply with Article 10.

What does Article 10 say?

Article 10 says:



“Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.”

This means you must either be processing the data in an official capacity, or have specific legal authorisation – which in the UK, is likely to mean a condition under the Data Protection Bill and compliance with the additional safeguards set out in the Bill. We will publish more detailed guidance on the conditions in the Bill once these provisions are finalised.

Even if you have a condition for processing offence data, you can only keep a comprehensive register of criminal convictions if you are doing so in an official capacity.

Further Reading

 [Relevant provisions in the GDPR - see Article 10](#) 

External link

 [Relevant provisions in the Data Protection Bill - See clauses 9 and 10, and Schedule 1](#) 

External link

Individual rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

This part of the guide explains these rights.

Right to be informed

At a glance

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
- You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. We call this 'privacy information'.
- You must provide privacy information to individuals at the time you collect their personal data from them.
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
- There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices.
- User testing is a good way to get feedback on how effective the delivery of your privacy information is.
- You must regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual's personal data to their attention before you start the processing.
- Getting the right to be informed correct can help you to comply with other aspects of the GDPR and build trust with people, but getting it wrong can leave you open to fines and lead to reputational damage.

Checklists

What to provide

We provide individuals with all the following privacy information:

- The name and contact details of our organisation.
- The name and contact details of our representative (if applicable).
- The contact details of our data protection officer (if applicable).
- The purposes of the processing.

- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

When to provide it

- We provide individuals with privacy information at the time we collect their personal data from them.

If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

- within a reasonable of period of obtaining the personal data and no later than one month;
- if we plan to communicate with the individual, at the latest, when the first communication takes place; or
- if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How to provide it

We provide the information in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and

- uses clear and plain language.

Changes to the information

- We regularly review and, where necessary, update our privacy information.
- If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information

- We undertake an information audit to find out what personal data we hold and what we do with it.
- We put ourselves in the position of the people we're collecting information about.
- We carry out user testing to evaluate how effective our privacy information is.

Best practice – delivering the information

When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

- a layered approach;
- dashboards;
- just-in-time notices;
- icons; and
- mobile and smart device functionalities.

In brief

- [What's new under the GDPR?](#)
- [What is the right to be informed and why is it important?](#)
- [What privacy information should we provide to individuals?](#)
- [When should we provide privacy information to individuals?](#)
- [How should we draft our privacy information?](#)
- [How should we provide privacy information to individuals?](#)
- [Should we test, review and update our privacy information?](#)

What's new under the GDPR?

The GDPR is more specific about the information you need to provide to people about what you do with their personal data.

You must actively provide this information to individuals in a way that is easy to access, read and understand.

You should review your current approach for providing privacy information to check it meets the standards of the GDPR.

What is the right to be informed and why is it important?

The right to be informed covers some of the key transparency requirements of the GDPR. It is about providing individuals with clear and concise information about what you do with their personal data.

Articles 13 and 14 of the GDPR specify what individuals have the right to be informed about. We call this 'privacy information'.

Using an effective approach can help you to comply with other aspects of the GDPR, foster trust with individuals and obtain more useful information from them.

Getting this wrong can leave you open to fines and lead to reputational damage.

What privacy information should we provide to individuals?

The table below summarises the information that you must provide. What you need to tell people differs slightly depending on whether you collect personal data from the individual it relates to or obtain it from another source.

What information do we need to provide?	Personal data collected from individuals	Personal data obtained from other sources
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓

The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓

When should we provide privacy information to individuals?

When you collect personal data from the individual it relates to, you must provide them with privacy information at the time you obtain their data.

When you obtain personal data from a source other than the individual it relates to, you need to provide the individual with privacy information:

- within a reasonable period of obtaining the personal data and no later than one month;
- if you use data to communicate with the individual, at the latest, when the first communication takes place; or
- if you envisage disclosure to someone else, at the latest, when you disclose the data.

You must actively provide privacy information to individuals. You can meet this requirement by putting the information on your website, but you must make individuals aware of it and give them an easy way to access it.

When collecting personal data from individuals, you do not need to provide them with any information that they already have.

When obtaining personal data from other sources, you do not need to provide individuals with privacy information if:

- the individual already has the information;
- providing the information to the individual would be impossible;
- providing the information to the individual would involve a disproportionate effort;
- providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
- you are required by law to obtain or disclose the personal data; or
- you are subject to an obligation of professional secrecy regulated by law that covers the personal data.

How should we draft our privacy information?

An information audit or data mapping exercise can help you find out what personal data you hold and what you do with it.

You should think about the intended audience for your privacy information and put yourself in their position.

If you collect or obtain children's personal data, you must take particular care to ensure that the information you provide them with is appropriately written, using clear and plain language.

For all audiences, you must provide information to them in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- uses clear and plain language.

How should we provide privacy information to individuals?

There are a number of techniques you can use to provide people with privacy information. You can use:

- **A layered approach** – short notices containing key privacy information that have additional layers of more detailed information.
- **Dashboards** – preference management tools that inform people how you use their data and allow them to manage what happens with it.
- **Just-in-time notices** – relevant and focused privacy information delivered at the time you collect individual pieces of information about people.
- **Icons** – small, meaningful, symbols that indicate the existence of a particular type of data processing.
- **Mobile and smart device functionalities** – including pop-ups, voice alerts and mobile device gestures.

Consider the context in which you are collecting personal data. It is good practice to use the same medium you use to collect personal data to deliver privacy information.

Taking a blended approach, using more than one of these techniques, is often the most effective way to provide privacy information.

Should we test, review and update our privacy information?

It is good practice to carry out user testing on your draft privacy information to get feedback on how easy it is to access and understand.

After it is finalised, undertake regular reviews to check it remains accurate and up to date.

If you plan to use personal data for any new purposes, you must update your privacy information and proactively bring any changes to people's attention.

The right to be informed in practice

If you **sell** personal data to (or **share** it with) other organisations:

- As part of the privacy information you provide, you must tell people who you are giving their information to, unless you are relying on an exception or an exemption.
- You can tell people the names of the organisations or the categories that they fall within; choose the option that is most meaningful.
- It is good practice to use a dashboard to let people manage who their data is sold to, or shared with, where they have a choice.

If you **buy** personal data from other organisations:

- You must provide people with your own privacy information, unless you are relying on an exception or an exemption.
- If you think that it is impossible to provide privacy information to individuals, or it would involve a disproportionate effort, you must carry out a DPIA to find ways to mitigate the risks of the processing.
- If your purpose for using the personal data is different to that for which it was originally obtained, you must tell people about this, as well as what your lawful basis is for the processing.
- Provide people with your privacy information within a reasonable period of buying the data, and no later than one month.

If you obtain personal data from **publicly accessible sources**:

- You still have to provide people with privacy information, unless you are relying on an exception or an exemption.
- If you think that it is impossible to provide privacy information to individuals, or it would involve a disproportionate effort, you must carry out a DPIA to find ways to mitigate the risks of the processing.
- Be very clear with individuals about any unexpected or intrusive uses of personal data, such as combining information about them from a number of different sources.
- Provide people with privacy information within a reasonable period of obtaining the data, and no later than one month.

If you apply **Artificial Intelligence (AI)** to personal data:

- Be upfront about it and explain your purposes for using AI.
- If the purposes for processing are unclear at the outset, give people an indication of what you are going to do with their data. As your processing purposes become clearer, update your privacy information and actively communicate this to people.
- Inform people about any new uses of personal data before you actually start the processing.
- If you use AI to make solely automated decisions about people with legal or similarly significant effects, tell them what information you use, why it is relevant and what the likely impact is going to be.

Consider using just-in-time notices and dashboards which can help to keep people informed and let them control further uses of their personal data.

Further Reading

 [Relevant provisions in the GDPR – See Articles 12-14, and Recitals 58 and 60-62](#) 

External link

In more detail – ICO guidance

We have published [detailed guidance on the right to be informed](#).

In more detail – Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

[WP29 guidelines on Transparency](#) 

Right of access

At a glance

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- You have one month to respond to a request.
- You cannot charge a fee to deal with a request in most circumstances.

Checklists

Preparing for subject access requests

- We know how to recognise a subject access request and we understand when the right of access applies.
- We have a policy for how to record requests we receive verbally.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.
- We understand the nature of the supplementary information we need to provide in response to a subject access request.

Complying with subject access requests

- We have processes in place to ensure that we respond to a subject access request without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to a request.
- We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.
- We understand what we need to consider if a request includes information about others.

In brief

What is the right of access?

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy

of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.

What is an individual entitled to?

Individuals have the right to obtain the following from you:

- confirmation that you are processing their personal data;
- a copy of their personal data; and
- other supplementary information – this largely corresponds to the information that you should provide in a privacy notice (see 'Supplementary information' below).

Personal data of the individual

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that you establish whether the information requested falls within the definition of personal data. For further information about the definition of personal data please see the [key definitions](#) guidance.

Other information

In addition to a copy of their personal data, you also have to provide individuals with the following information:

- the purposes of your processing;
- the categories of personal data concerned;
- the recipients or categories of recipient you disclose the personal data to;
- your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards you provide if you transfer personal data to a third country or international organisation.

You may be providing much of this information already in your privacy notice.

How do we recognise a request?

The GDPR does not specify how to make a valid request. Therefore, an individual can make a subject access request to you verbally or in writing. It can also be made to any part of your organisation (including by social media) and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'subject access request' or Article 15 of the GDPR, as

long as it is clear that the individual is asking for their own personal data.

This presents a challenge as any of your employees could receive a valid request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Should we provide a specially designed form for individuals to make a subject access request?

Standard forms can make it easier both for you to recognise a subject access request and for the individual to include all the details you might need to locate the information they want.

Recital 59 of the GDPR recommends that organisations 'provide means for requests to be made electronically, especially where personal data are processed by electronic means'. You should therefore consider designing a subject access form that individuals can complete and submit to you electronically.

However, even if you have a form, you should note that a subject access request is valid if it is submitted by any means, so you will still need to comply with any requests you receive in a letter, a standard email or verbally.

Therefore, although you may invite individuals to use a form, you must make it clear that it is not compulsory and do not try to use this as a way of extending the one month time limit for responding.

How should we provide the data to individuals?

If an individual makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise.

The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63). This will not be appropriate for all organisations, but there are some sectors where this may work well.

However, providing remote access should not adversely affect the rights and freedoms of others – including trade secrets or intellectual property.

We have received a request but need to amend the data before sending out the response. Should we send out the “old” version?

It is our view that a subject access request relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted while you are dealing with the request. So it would be reasonable for you to supply information you hold when you send out a response, even if this is different to that held when you received the request.

However, it is not acceptable to amend or delete the data if you would not otherwise have done so. Under the DP Bill, it is an offence to make any amendment with the intention of preventing its

disclosure.

Do we have to explain the contents of the information we send to the individual?

The GDPR requires that the information you provide to an individual is in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This will be particularly important where the information is addressed to a child.

At its most basic, this means that the additional information you provide in response to a request (see the 'Other information' section above) should be capable of being understood by the average person (or child). However, you are not required to ensure that the information is provided in a form that can be understood by the particular individual making the request.

For further information about requests made by a child please see the 'What about requests for information about children?' section below.

Example

An individual makes a request for their personal data. When preparing the response, you notice that a lot of it is in coded form. For example, attendance at a particular training session is logged as "A", while non-attendance at a similar event is logged as "M". Also, some of the information is in the form of handwritten notes that are difficult to read. Without access to your key or index to explain this information, it would be impossible for anyone outside your organisation to understand. In this case, you are required to explain the meaning of the coded information. However, although it is good practice to do so, you are not required to decipher the poorly written notes, as the GDPR does not require you to make information legible.

Example

You receive a subject access request from someone whose English comprehension skills are quite poor. You send a response and they ask you to translate the information you sent them. You are not required to do this even if the person who receives it cannot understand all of it because it can be understood by the average person. However, it is good practice for you to help individuals understand the information you hold about them.

Can we charge a fee?

In most cases you cannot charge a fee to comply with a subject access request.

However, as noted above, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

You can also charge a reasonable fee if an individual requests further copies of their data following a

request. You must base the fee on the administrative costs of providing further copies.

How long do we have to comply?

You must act on the subject access request without undue delay and at the latest within one month of receipt.

You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality.

You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information.

What about requests for large amounts of personal data?

If you process a large amount of information about an individual you can ask them for more information to clarify their request. You should only ask for information that you reasonably need to find the personal data covered by the request.

You need to let the individual know as soon as possible that you need more information from them before responding to their request. The period for responding to the request begins when you receive the additional information. However, if an individual refuses to provide any additional information, you must still endeavour to comply with their request ie by making reasonable searches for the information covered by the request.

What about requests made on behalf of others?

The GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

Example

A building society has an elderly customer who visits a particular branch to make weekly withdrawals from one of her accounts. Over the past few years, she has always been accompanied by her daughter who is also a customer of the branch. The daughter makes a subject access request on behalf of her mother and explains that her mother does not feel up to making the request herself as she does not understand the ins and outs of data protection. As the information held by the building society is mostly financial, it is rightly cautious about giving customer information to a third party. If the daughter had a general power of attorney, the society would be happy to comply. They ask the daughter whether she has such a power, but she does not.

Bearing in mind that the branch staff know the daughter and have some knowledge of the

relationship she has with her mother, they might consider complying with the request by making a voluntary disclosure. However, the building society is not obliged to do so, and it would not be unreasonable to require more formal authority.

If you think an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

There are cases where an individual does not have the mental capacity to manage their own affairs. Although there are no specific provisions in the GDPR, the Mental Capacity Act 2005 or in the Adults with Incapacity (Scotland) Act 2000 enabling a third party to exercise subject access rights on behalf of such an individual, it is reasonable to assume that an attorney with authority to manage the property and affairs of an individual will have the appropriate authority. The same applies to a person appointed to make decisions about such matters:

- in England and Wales, by the Court of Protection;
- in Scotland, by the Sheriff Court; and
- in Northern Ireland, by the High Court (Office of Care and Protection).

What about requests for information about children?

Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information

about them.

In Scotland, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. This presumption does not apply in England and Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases.

For further information on situations where the request has been made by a child, see our [guidance on children and the GDPR](#).

What about data held by credit reference agencies?

In the draft DP Bill there are special provisions about the access to personal data held by credit reference agencies. Unless otherwise specified, a subject access request to a credit reference agency only applies to information relating to the individual's financial standing. Credit reference agencies must also inform individuals of their rights under s.159 of the Consumer Credit Act. Once the DP Bill is finalised, we will update our guidance accordingly.

What should we do if the data includes information about other people?

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual.

The DP Bill says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, you must take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

For the avoidance of doubt, you cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the individual who is the subject of the request and information about someone else.

Once the DP Bill is finalised, we will update our guidance accordingly.

If we use a processor, does this mean they would have to deal with any subject access requests we receive?

Responsibility for complying with a subject access request lies with you as the controller. You need to ensure that you have contractual arrangements in place to guarantee that subject access requests are dealt with properly, irrespective of whether they are sent to you or to the processor. More information about contracts and liabilities between controllers and processors can be found [here](#).

You are not able to extend the one month time limit on the basis that you have to rely on a processor to provide the information that you need to respond. As mentioned above, you can only extend the time limit by two months if the request is complex or you have received a number of requests from the individual.

Can we refuse to comply with a request?

You can refuse to comply with a subject access request if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case you need to justify your decision.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

In more detail – Data Protection Bill

There are other proposed exemptions from the right of access that are contained in the draft DP Bill. As proposed, these exemptions will apply in certain circumstances, broadly associated with why you are processing the data. Once the DP Bill is finalised, we will update our guidance accordingly, and provide further detail on the application of these exemptions.

What should we do if we refuse to comply with a request?

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information

to identify the individual.

Can I require an individual to make a subject access request?

In the draft DP bill it is a criminal offence, in certain circumstances and in relation to certain information, to require an individual to make a subject access request. Once the DP Bill is finalised, we will update our guidance accordingly, and provide further detail on this offence.

Further Reading

 [Relevant provisions in the GDPR - See Articles 12, 15 and Recitals 63, 64](#) 

External link

Right to rectification

At a glance

- The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- You have one calendar month to respond to a request.
- In certain circumstances you can refuse a request for rectification.
- This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).

Checklists

Preparing for requests for rectification

- We know how to recognise a request for rectification and we understand when this right applies.
- We have a policy for how to record requests we receive verbally.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for rectification

- We have processes in place to ensure that we respond to a request for rectification without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to a request.
- We have appropriate systems to rectify or complete information, or provide a supplementary statement.
- We have procedures in place to inform any recipients if we rectify any data we have shared with them.

In brief

What is the right to rectification?

Under Article 16 of the GDPR individuals have the right to have inaccurate personal data rectified. An

individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the GDPR (Article 5(1)(d)). However, although you may have already taken steps to ensure that the personal data was accurate when you obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

What do we need to do?

If you receive a request for rectification you should take reasonable steps to satisfy yourself that the data is accurate and to rectify the data if necessary. You should take into account the arguments and evidence provided by the data subject.

What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort you should put into checking its accuracy and, if necessary, taking steps to rectify it. For example, you should make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

You may also take into account any steps you have already taken to verify the accuracy of the data prior to the challenge by the data subject.

When is data inaccurate?

The GDPR does not give a definition of the term accuracy. However, the Data Protection Bill states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

What should we do about data that records a mistake?

Determining whether personal data is inaccurate can be more complex if the data refers to a mistake that has subsequently been resolved. It may be possible to argue that the record of the mistake is, in itself, accurate and should be kept. In such circumstances the fact that a mistake was made and the correct information should also be included in the individuals data.

Example

If a patient is diagnosed by a GP as suffering from a particular illness or condition, but it is later proved that this is not the case, it is likely that their medical records should record both the initial diagnosis (even though it was later proved to be incorrect) and the final findings. Whilst the medical record shows a misdiagnosis, it is an accurate record of the patient's medical treatment. As long as the medical record contains the up-to-date findings, and this is made clear in the record, it would be difficult to argue that the record is inaccurate and should be rectified.

What should we do about data that records a disputed opinion?

It is also complex if the data in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

What should we do while we are considering the accuracy?

Under Article 18 an individual has the right to request restriction of the processing of their personal data where they contest its accuracy and you are checking it. As a matter of good practice, you should restrict the processing of the personal data in question whilst you are verifying its accuracy, whether or not the individual has exercised their right to restriction. For more information, see our [guidance on the right to restriction](#).

What should we do if we are satisfied that the data is accurate?

You should let the individual know if you are satisfied that the personal data is accurate, and tell them that you will not be amending the data. You should explain your decision, and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

It is also good practice to place a note on your system indicating that the individual challenges the accuracy of the data and their reasons for doing so.

Can we refuse to comply with the request for rectification for other reasons?

You can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case you will need to justify your decision.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual without undue delay and within one month. You do not need to comply with the request until you have received the fee.

In more detail – Data Protection Bill

There are other proposed exemptions from the right to rectification that are contained in the draft DP Bill. As proposed, these exemptions will apply in certain circumstances, broadly associated with why you are processing the data. Once the DP Bill is finalised, we will update our guidance accordingly, and provide further detail on the application of these exemptions.

What should we do if we refuse to comply with a request for rectification?

You must inform the individual without undue delay and within one month of receipt of the request about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How can we recognise a request?

The GDPR does not specify how to make a valid request. Therefore, an individual can make a request for rectification verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request to rectify personal data does not need to mention the phrase 'request for rectification' or Article 16 of the GDPR to be a valid request. As long as the individual has challenged the accuracy of their data and has asked you to correct it, or has asked that you take steps to complete data held about them that is incomplete, this will be a valid request under Article 16.

This presents a challenge as any of your employees could receive a valid verbal request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Can we charge a fee?

No, in most cases you cannot charge a fee to comply with a request for rectification.

However, as noted above, if the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

You must act upon the request without undue delay and at the latest within one month of receipt.

You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the next day (4

September). This gives the organisation until 4 October to comply with the request.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time to respond to a request?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

The circumstances in which you can extend the time to respond can include further consideration of the accuracy of disputed data - although you can only do this in complex cases - and the result may be that at the end of the extended time period you inform the individual that you consider the data in question to be accurate.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You must let the individual know without undue delay and within one month that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Do we have to tell other organisations if we rectify personal data?

If you have disclosed the personal data to others, you must contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Further Reading

 [Relevant provisions in the GDPR - See Articles 5, 12, 16 and 19](#) 

External link

Right to erasure

At a glance

- The GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- Individuals can make a request for erasure verbally or in writing.
- You have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- This right is not the only way in which the GDPR places an obligation on you to consider whether to delete personal data.

Checklists

Preparing for requests for erasure

- We know how to recognise a request for erasure and we understand when the right applies.
- We have a policy for how to record requests we receive verbally.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for erasure

- We have processes in place to ensure that we respond to a request for erasure without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to a request.
- We understand that there is a particular emphasis on the right to erasure if the request relates to data collected from children.
- We have procedures in place to inform any recipients if we erase any data we have shared with them.
- We have appropriate methods in place to erase information.

In brief

What is the right to erasure?

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

How does the right to erasure apply to data collected from children?

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR.

Therefore, if you process data collected from children, you should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

For further details about the right to erasure and children's personal data please read our guidance on [children's privacy](#).

Do we have to tell other organisations about the erasure of personal data?

The GDPR specifies two circumstances where you should tell other organisations about the erasure of personal data:

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).

If you have disclosed the personal data to others, you must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients.

The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Where personal data has been made public in an online environment reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable you should take into account available technology and the cost of implementation.

When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine (eg where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

For more information about special categories of data please see our [Guide to the GDPR](#).

Can we refuse to comply with a request for other reasons?

You can refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case you will need to justify your decision.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

In more detail – Data Protection Bill

There are other proposed exemptions from the right to erasure that are contained in the draft DP Bill. As proposed, these exemptions will apply in certain circumstances, broadly associated with why you are processing the data. Once the DP Bill is finalised, we will update our guidance accordingly, and provide further detail on the application of these exemptions.

What should we do if we refuse to comply with a request for erasure?

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How do we recognise a request?

The GDPR does not specify how to make a valid request. Therefore, an individual can make a request for erasure verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'request for erasure' or Article 17 of the GDPR, as long as one of the conditions listed above apply.

This presents a challenge as any of your employees could receive a valid verbal request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Can we charge a fee?

No, in most cases you cannot charge a fee to comply with a request for erasure.

However, as noted above, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

You must act upon the request without undue delay and at the latest within one month of receipt.

You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request is made.

Example

An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You must let the individual know without undue delay and within one month that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Further Reading

 [Relevant provisions in the GDPR - See Articles 6, 9, 12, 17 and Recitals 65, 66](#) 

External link

Right to restrict processing

At a glance

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, you are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- You have one calendar month to respond to a request.
- This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Checklists

Preparing for requests for restriction

- We know how to recognise a request for restriction and we understand when the right applies.
- We have a policy in place for how to record requests we receive verbally.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for restriction

- We have processes in place to ensure that we respond to a request for restriction without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to a request.
- We have appropriate methods in place to restrict the processing of personal data on our systems.
- We have appropriate methods in place to indicate on our systems that further processing has been restricted.
- We understand the circumstances when we can process personal data that has been restricted.
- We have procedures in place to inform any recipients if we restrict any data we have shared with them.
- We understand that we need to tell individuals before we lift a restriction on processing.

In brief

What is the right to restrict processing?

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

When does the right to restrict processing apply?

Individuals have the right to request you restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

Although this is distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing:

- if an individual has challenged the accuracy of their data and asked for you to rectify it (Article 16), they also have a right to request you restrict processing while you consider their rectification request; or
- if an individual exercises their right to object under Article 21(1), they also have a right to request you restrict processing while you consider their objection request.

Therefore, as a matter of good practice you should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question.

How do we restrict processing?

You need to have processes in place that enable you to restrict personal data if required. It is important to note that the definition of processing includes a broad range of operations including collection, structuring, dissemination and erasure of data. Therefore, you should use methods of restriction that are appropriate for the type of processing you are carrying out.

The GDPR suggests a number of different methods that could be used to restrict data, such as:

- temporarily moving the data to another processing system;

- making the data unavailable to users; or
- temporarily removing published data from a website.

It is particularly important that you consider how you store personal data that you no longer need to process but the individual has requested you restrict (effectively requesting that you do not erase the data).

If you are using an automated filing system, you need to use technical measures to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. You should also note on your system that the processing of this data has been restricted.

Can we do anything with restricted data?

You must not process the restricted data in any way **except to store it** unless:

- you have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

Do we have to tell other organisations about the restriction of personal data?

Yes. If you have disclosed the personal data in question to others, you must contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

When can we lift the restriction?

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

- the individual has disputed the accuracy of the personal data and you are investigating this; or
- the individual has objected to you processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of your legitimate interests, and you are considering whether your legitimate grounds override those of the individual.

Once you have made a decision on the accuracy of the data, or whether your legitimate grounds override those of the individual, you may decide to lift the restriction.

If you do this, you must inform the individual **before** you lift the restriction.

As noted above, these two conditions are linked to the right to rectification (Article 16) and the right to object (Article 21). This means that if you are informing the individual that you are lifting the restriction (on the grounds that you are satisfied that the data is accurate, or that your legitimate grounds override theirs) you should also inform them of the reasons for your refusal to act upon their rights under Articles 16 or 21. You will also need to inform them of their right to make a complaint to the ICO or another

supervisory authority; and their ability to seek a judicial remedy.

Can we refuse to comply with a request for restriction?

You can refuse to comply with a request for restriction if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case you will need to justify your decision.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

In more detail – Data Protection Bill

There are other proposed exemptions from the right to restriction that are contained in the draft DP Bill. As proposed, these exemptions will apply in certain circumstances, broadly associated with why you are processing the data. Once the DP Bill is finalised, we will update our guidance accordingly, and provide further detail on the application of these exemptions.

What should we do if we refuse to comply with a request for restriction?

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How do we recognise a request?

The GDPR does not specify how to make a valid request. Therefore, an individual can make a request for restriction verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'request for restriction' or Article 18 of the GDPR, as long as one of the conditions listed above apply.

This presents a challenge as any of your employees could receive a valid verbal request. However, you

have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

Can we charge a fee?

No, in most cases you cannot charge a fee to comply with a request for restriction.

However, as noted above, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

You must act upon the request without undue delay and at the latest within one month of receipt.

You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You must let the individual know without undue delay and within one month that you need more information from them to confirm their identity. You do not need to comply with the request until you have received the additional information.

Further Reading

 [Relevant provisions in the GDPR - See Articles 18, 19 and Recital 67](#) 

External link

Right to data portability

At a glance

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to information an individual has provided to a controller.
- Some organisations in the UK already offer data portability through midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.

Checklists

Preparing for requests for data portability

- We know how to recognise a request for data portability and we understand when the right applies.
- We have a policy for how to record requests we receive verbally.
- We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for data portability

- We can transmit personal data in structured, commonly used and machine readable formats.
- We use secure methods to transmit personal data.
- We have processes in place to ensure that we respond to a request for data portability without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to a request.

In brief

What is the right to data portability?

The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

When does the right apply?

The right to data portability only applies when:

- your lawful basis for processing this information is consent **or** for the performance of a contract; and
- you are carrying out the processing by automated means (ie excluding paper files).

What does the right apply to?

Information is only within the scope of the right to data portability if it is personal data of the individual that they have provided to you.

What does 'provided to a controller' mean?

Sometimes the personal data an individual has provided to you will be easy to identify (eg their mailing address, username, age). However, the meaning of data 'provided to' you is not limited to this. It is also personal data resulting from observation of an individual's activities (eg where using a device or service).

This may include:

- history of website usage or search activities;
- traffic and location data; or
- 'raw' data processed by connected objects such as smart meters and wearable devices.

It does not include any additional data that you have created based on the data an individual has provided to you. For example, if you use the data they have provided to create a user profile then this data would not be in scope of data portability.

You should however note that if this 'inferred' or 'derived' data is personal data, you still need to provide it to an individual if they make a subject access request. Bearing this in mind, if it is clear that the individual is seeking access to the inferred/derived data, as part of a wider portability request, it would be good practice to include this data in your response.

Does the right apply to anonymous or pseudonymous data?

The right to data portability only applies to personal data. This means that it does not apply to genuinely anonymous data. However, pseudonymous data that can be clearly linked back to an individual (eg where that individual provides the respective identifier) is within scope of the right.

What happens if the personal data includes information about others?

If the requested information includes information about others (eg third party data) you need to consider whether transmitting that data would adversely affect the rights and freedoms of those third parties.

Generally speaking, providing third party data to the individual making the portability request should not be a problem, assuming that the requestor provided this data to you within their information in the first place. However, you should always consider whether there will be an adverse effect on the rights and freedoms of third parties, in particular when you are transmitting data directly to another controller.

If the requested data has been provided to you by multiple data subjects (eg a joint bank account) you need to be satisfied that all parties agree to the portability request. This means that you may have to seek agreement from all the parties involved.

What is an individual entitled to?

The right to data portability entitles an individual to:

- receive a copy of their personal data; and/or
- have their personal data transmitted from one controller to another controller.

Individuals have the right to receive their personal data and store it for further personal use. This allows the individual to manage and reuse their personal data. For example, an individual wants to retrieve their contact list from a webmail application to build a wedding list or to store their data in a personal data store.

You can achieve this by either:

- directly transmitting the requested data to the individual; or
- providing access to an automated tool that allows the individual to extract the requested data themselves.

This does not create an obligation for you to allow individuals more general and routine access to your systems – only for the extraction of their data following a portability request.

You may have a preferred method of providing the information requested depending on the amount and complexity of the data requested. In either case, you need to ensure that the method is secure.

What are the limits when transmitting personal data to another controller?

Individuals have the right to ask you to transmit their personal data directly to another controller without hindrance. If it is technically feasible, you should do this.

You should consider the **technical feasibility** of a transmission on a request by request basis. The right to data portability does not create an obligation for you to adopt or maintain processing systems which are technically compatible with those of other organisations (GDPR Recital 68). However, you should take a reasonable approach, and this should not generally create a barrier to transmission.

Without hindrance means that you should not put in place any legal, technical or financial obstacles which slow down or prevent the transmission of the personal data to the individual, or to another organisation.

However, there may be legitimate reasons why you cannot undertake the transmission. For example, if the transmission would adversely affect the rights and freedoms of others. It is however your responsibility to justify why these reasons are legitimate and why they are not a 'hindrance' to the transmission.

Do we have responsibility for the personal data we transmit to others?

If you provide information directly to an individual or to another organisation in response to a data portability request, you are not responsible for any subsequent processing carried out by the individual or the other organisation. However, you are responsible for the transmission of the data and need to take appropriate measures to ensure that it is transmitted securely and to the right destination.

If you provide data to an individual, it is possible that they will store the information in a system with less security than your own. Therefore, you should make individuals aware of this so that they can take steps to protect the information they have received.

You also need to ensure that you comply with the other provisions in the GDPR. For example, whilst there is no specific obligation under the right to data portability to check and verify the quality of the data you transmit, you should already have taken reasonable steps to ensure the accuracy of this data in order to comply with the requirements of the accuracy principle of the GDPR.

How should we provide the data?

You should provide the personal data in a format that is:

- structured;
- commonly used; and
- machine-readable.

Although these terms are not defined in the GDPR these three characteristics can help you decide whether the format you intend to use is appropriate.

You can also find relevant information in the 'Open Data Handbook', published by Open Knowledge International. The handbook is a guide to 'open data', information that is free to access and can be re-used for any purpose – particularly information held by the public sector. The handbook contains a number of definitions that are relevant to the right to data portability, and this guidance includes some of these below.

What does 'structured' mean?

Structured data allows for easier transfer and increased usability.

The Open Data Handbook defines 'structured data' as:



'data where the structural relation between elements is explicit in the way the data is stored on a computer disk.'

This means that software must be able to extract specific elements of the data. An example of a structured format is a spreadsheet, where the data is organised into rows and columns, ie it is 'structured'. In practice, some of the personal data you process will already be in structured form.

In many cases, if a format is structured it is also machine-readable.

What does ‘commonly used’ mean?

This simply means that the format you choose must be widely-used and well-established.

However, just because a format is ‘commonly used’ does not mean it is appropriate for data portability. You have to consider whether it is ‘structured’, and ‘machine-readable’ as well. Although you may be using common software applications, which save data in commonly-used formats, these may not be sufficient to meet the requirements of data portability.

What does ‘machine-readable’ mean?

The Open Data Handbook states that ‘machine readable’ data is:



‘Data in a data format that can be automatically read and processed by a computer.’

Furthermore, Regulation 2 of the Re-use of Public Sector Information Regulations 2015 defines ‘machine-readable format’ as:



‘A file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure.’

Machine-readable data can be made directly available to applications that request that data over the web. This is undertaken by means of an application programming interface (“API”).

If you are able to implement such a system then you can facilitate data exchanges with individuals and respond to data portability requests in an easy manner.

Should we use an ‘interoperable’ format?

Although you are not required to use an interoperable format, this is encouraged by the GDPR, which seeks to promote the concept of interoperability. Recital 68 says:



‘Data controllers should be encouraged to develop interoperable formats that enable data portability.’

Interoperability allows different systems to share information and resources. An ‘interoperable format’ is a type of format that allows data to be exchanged between different systems and be understandable to both.

At the same time, you are not expected to maintain systems that are technically compatible with those of other organisations. Data portability is intended to produce interoperable systems, not compatible ones.

What formats can we use?

You may already be using an appropriate format within your networks and systems, and/or you may be required to use a particular format due to the particular industry or sector you are part of. Provided it meets the requirements of being structured, commonly-used and machine readable then it could be appropriate for a data portability request.

The GDPR does not require you to use open formats internally. Your processing systems may indeed use proprietary formats which individuals may not be able to access if you provide data to them in these formats. In these cases you need to perform some additional processing on the personal data in order to put it into the type of format required by the GDPR.

Where no specific format is in common use within your industry or sector, you should provide personal data using open formats such as CSV, XML and JSON. You may also find that these formats are the easiest for you to use when answering data portability requests.

For further information on CSV, XML and JSON, please see below.

What is CSV?

CSV stands for 'Comma Separated Values'. It is defined by the Open Data Handbook as:



'a standard format for spreadsheet data. Data is represented in a plain text file, with each data row on a new line and commas separating the values on each row. As a very simple open format it is easy to consume and is widely used for publishing open data.'

CSV is used to exchange data and is widely supported by software applications. Although CSV is not standardised it is nevertheless structured, commonly used and machine-readable and is therefore an appropriate format for you to use when responding to a data portability request.

What is XML?

XML stands for 'Extensible Markup Language'. It is defined by the Open Data Handbook as:



'a simple and powerful standard for representing structured data.'

It is a file format that is intended to be both human readable and machine-readable. Unlike CSV, XML is defined by a set of open standards maintained by the World Wide Web Consortium ("W3C"). It is widely used for documents, but can also be used to represent data structures such as those used in web

services.

This means XML can be processed by APIs, facilitating data exchange. For example, you may develop or implement an API to exchange personal data in XML format with another organisation. In the context of data portability, this can allow you to transmit personal data to an individual's personal data store, or to another organisation if the individual has asked you to do so.

What is JSON?

JSON stands for 'JavaScript Object Notation'. The Open Data Handbook defines JSON as:



'a simple but powerful format for data. It can describe complex data structures, is highly machine-readable as well as reasonably human-readable, and is independent of platform and programming language, and is therefore a popular format for data interchange between programs and systems.'

It is a file format based on the JavaScript language that many web sites use and is used as a data interchange format. As with XML, it can be read by humans or machines. It is also a standardised open format maintained by the W3C.

Are these the only formats we can use?

CSV, XML and JSON are three examples of structured, commonly used and machine-readable formats that are appropriate for data portability. However, this does not mean you are obliged to use them. Other formats exist that also meet the requirements of data portability.

Example

The RDF or 'Resource Description Framework' format is also a structured, commonly-used, machine-readable format. It is an open standard published by the W3C and is intended to provide interoperability between applications exchanging information.

You should however consider the nature of the portability request. If the individual cannot make use of the format, even if it is structured, commonly-used and machine-readable then the data will be of no use to them.

Further reading

The Open Data Handbook is published by Open Knowledge International and is a guide to 'open data'. The Handbook is updated regularly and you can read it here:

<http://opendatahandbook.org>

W3C candidate recommendation for XML is available here:

<http://www.w3.org/TR/2008/REC-xml-20081126/>

W3C's specification of the JSON data interchange format is available here:

<https://tools.ietf.org/html/rfc7159>

W3C's list of specifications for RDF is available here:

http://www.w3.org/standards/techs/rdf#w3c_all

What responsibilities do we have when we receive personal data because of a data portability request?

When you receive personal data that has been transmitted as part of a data portability request, you need to process this data in line with data protection requirements.

In deciding whether to accept and retain personal data, you should consider whether the data is relevant and not excessive in relation to the purposes for which you will process it. You also need to consider whether the data contains any third party information.

As a new controller, you need to ensure that you have an appropriate lawful basis for processing any third party data and that this processing does not adversely affect the rights and freedoms of those third parties. If you have received personal data which you have no reason to keep, you should delete it as soon as possible. When you accept and retain data, it becomes your responsibility to ensure that you comply with the requirements of the GDPR.

In particular, if you receive third party data you should not use this for your own purposes. You should keep the third party data under the sole control of the individual who has made the portability request, and only used for their own purposes.

Example

An individual enters into a contract with a controller for the provision of a service. The controller relies on Article 6(1)(b) to process the individual's personal data. The controller receives information from a data portability request that includes information about third parties. The controller has a legitimate interest to process the third party data under Article 6(1)(f) so that it can provide this service to the individual. However, it should not then use this data to send direct marketing to the third parties.

When can we refuse to comply with a request for data portability?

You can refuse to comply with a request for data portability if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request; or

- refuse to deal with the request.

In either case you will need to justify your decision.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

In more detail – Data Protection Bill

There are other proposed exemptions from the right to data portability that are contained in the draft DP Bill. As proposed, these exemptions will apply in certain circumstances, broadly associated with why you are processing the data. Once the DP Bill is finalised, we will update our guidance accordingly, and provide further detail on the application of these exemptions.

What should we do if we refuse to comply with a request for data portability?

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How do we recognise a request?

The GDPR does not specify how individuals should make data portability requests. Therefore, requests could be made verbally or in writing. They can also be made to any part of your organisation and do not have to be to a specific person or contact point.

A request does not have to include the phrase 'request for data portability' or a reference to 'Article 20 of the GDPR', as long as one of the conditions listed above apply.

This presents a challenge as any of your employees could receive a valid request. However, you have a legal responsibility to identify that an individual has made a request to you and handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Additionally, it is good practice to have a policy for recording details of the requests you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the request. We also recommend that you keep a log of verbal requests.

In practice, you may already have processes in place to enable your staff to recognise subject access requests, such as training or established procedures. You could consider adapting them to ensure your

staff also recognise data portability requests.

Can we charge a fee?

No, in most cases you cannot charge a fee to comply with a request for data portability.

However, as noted above, if the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

You must act upon the request without undue delay and at the latest within one month of receipt.

You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

Example

An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

Can we extend the time for a response?

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information.

Further Reading

 [Relevant provisions in the GDPR - See Articles 13, 20 and Recital 68](#) 

External link

In more detail – Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party has published [guidelines](#) and [FAQs](#) on data portability for organisations.

Right to object

At a glance

- The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies you may be able to continue processing if you can show that you have a compelling reason for doing so.
- You must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.
- You have one calendar month to respond to an objection.

Checklists

Preparing for objections to processing

- We know how to recognise an objection and we understand when the right applies.
- We have a policy in place for how to record objections we receive verbally.
- We understand when we can refuse an objection and are aware of the information we need to provide to individuals when we do so.
- We have clear information in our privacy notice about individuals' right to object, which is presented separately from other information on their rights.
- We understand when we need to inform individuals of their right to object in addition to including it in our privacy notice.

Complying with requests which object to processing

- We have processes in place to ensure that we respond to an objection without undue delay and within one month of receipt.
- We are aware of the circumstances when we can extend the time limit to respond to an objection.
- We have appropriate methods in place to erase, suppress or otherwise cease processing personal data.

In brief

What is the right to object?

Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask you to stop processing their personal data.

The right to object only applies in certain circumstances. Whether it applies depends on your purposes for processing and your lawful basis for processing.

When does the right to object apply?

Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

Individuals can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in you; or
- your legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute.

If you are processing data for scientific or historical research, or statistical purposes, the right to object is more limited.

These various grounds are discussed further below.

Direct marketing

An individual can ask you to stop processing their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing.

This is an absolute right and there are no exemptions or grounds for you to refuse. Therefore, when you receive an objection to processing for direct marketing, you must stop processing the individual's data for this purpose.

However, this does not automatically mean that you need to erase the individual's personal data, and in most cases it will be preferable to suppress their details. Suppression involves retaining just enough information about them to ensure that their preference not to receive direct marketing is respected in future.

Processing based upon public task or legitimate interests

An individual can also object where you are relying on one of the following lawful bases:

- 'public task' (for the performance of a task carried out in the public interest),
- 'public task' (for the exercise of official authority vested in you), or
- legitimate interests.

An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation.

In these circumstances this is not an absolute right, and you can continue processing if:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

If you are deciding whether you have compelling legitimate grounds which override the interests of an individual, you should consider the reasons why they have objected to the processing of their data. In particular, if an individual objects on the grounds that the processing is causing them substantial damage or distress (eg the processing is causing them financial loss), the grounds for their objection will have more weight. In making a decision on this, you need to balance the individual's interests, rights and freedoms with your own legitimate grounds. During this process you should remember that the responsibility is for you to be able to demonstrate that your legitimate grounds override those of the individual.

If you are satisfied that you do not need to stop processing the personal data in question you should let the individual know. You should explain your decision, and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

Research purposes

Where you are processing personal data for scientific or historical research, or statistical purposes, the right to object is more restricted.

Article 21(4) states:



'Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her personal situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.'

Effectively this means that if you are processing data for these purposes and have appropriate safeguards in place (eg data minimisation and pseudonymisation where possible) the individual only has a right to object if your lawful basis for processing is:

- public task (on the basis that it is necessary for the exercise of official authority vested in you), or
- legitimate interests.

The individual does not have a right to object if your lawful basis for processing is public task because it is necessary for the performance of a task carried out in the public interest.

Article 21(4) therefore differentiates between the two parts of the [public task lawful basis](#) (performance of a task carried out in the public interest **or** in the exercise of official authority vested in you).

This may cause difficulties if you are relying on the public task lawful basis for processing. It may not always be clear whether you are carrying out the processing solely as a task in the public interest, or in

the exercise of official authority. Indeed, it may be difficult to differentiate between the two.

As such, it is good practice that if you are relying upon the public task lawful basis and receive an objection, you should consider the objection on its own merits and go on to consider the steps outlined in the next paragraph, rather than refusing it outright. If you do intend to refuse an objection on the basis that you are carrying out research or statistical work solely for the performance of a public task carried out in the public interest you should be clear in your privacy notice that you are only carrying out this processing on this basis.

If you do receive an objection you may be able to continue processing, if you can demonstrate that you have a compelling legitimate reason or the processing is necessary for legal claims. You need to go through the steps outlined in the previous section to demonstrate this.

As noted above, if you are satisfied that you do not need to stop processing you should let the individual know. You should provide an explanation for your decision, and inform them of their right to make a complaint to the ICO or another supervisory authority, as well as their ability to seek to enforce their rights through a judicial remedy.

Do we need to tell individuals about the right to object?

The GDPR is clear that you must inform individuals of their right to object at the latest at the time of your first communication with them where:

- you process personal data for direct marketing purposes, or
- your lawful basis for processing is:
 - public task (for the performance of a task carried out in the public interest),
 - public task (for the exercise of official authority vested in you), or
 - legitimate interests.

If one of these conditions applies, you should explicitly bring the right to object to the individual's attention. You should present this information clearly and separately from any other information.

If you are processing personal data for research or statistical purposes you should include information about the right to object (along with information about the other rights of the individual) in your privacy notice.

Do we always need to erase personal data to comply with an objection?

Where you have received an objection to the processing of personal data and you have no grounds to refuse, you need to stop processing the data.

This may mean that you need to erase personal data as the definition of processing under the GDPR is broad, and includes storing data. However, as noted above, this will not always be the most appropriate action to take.

Erasure may not be appropriate if you process the data for other purposes as you need to retain the data for those purposes. For example, when an individual objects to the processing of their data for direct marketing, you can place their details onto a suppression list to ensure that you continue to comply with their objection. However, you need to ensure that the data is clearly marked so that it is not processed for purposes the individual has objected to.

Can we refuse to comply with an objection for other reasons?

You can also refuse to comply with an objection if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If you consider that an objection is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with it; or
- refuse to deal with it.

In either case you will need to justify your decision.

You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

In more detail – Data Protection Bill

There are other proposed exemptions from the right to object that are contained in the draft DP Bill. As proposed, these exemptions will apply in certain circumstances, broadly associated with why you are processing the data. Once the DP Bill is finalised, we will update our guidance accordingly, and provide further detail on the application of these exemptions.

What should we do if we refuse to comply with an objection?

You must inform the individual without undue delay and within one month of receipt of the request.

You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual.

How do we recognise an objection?

The GDPR does not specify how to make a valid objection. Therefore, an objection to processing can be made verbally or in writing. It can also be made to any part of your organisation and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'objection to processing' or Article 21 of the GDPR - as long as one of the conditions listed above apply.

This presents a challenge as any of your employees could receive a valid verbal objection. However, you have a legal responsibility to identify that an individual has made an objection to you and to handle it accordingly. Therefore you may need to consider which of your staff who regularly interact with individuals may need specific training to identify an objection.

Additionally, it is good practice to have a policy for recording details of the objections you receive, particularly those made by telephone or in person. You may wish to check with the requester that you have understood their request, as this can help avoid later disputes about how you have interpreted the objection. We also recommend that you keep a log of verbal objections.

Can we charge a fee?

No, in most cases you cannot charge a fee to comply with an objection to processing.

However, as noted above, where the objection is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

How long do we have to comply?

You must act upon the objection without undue delay and at the latest within one month of receipt.

You should calculate the time limit from the day after you receive the objection (whether the day after is a working day or not) until the corresponding calendar date in the next month.

Example

An organisation receives an objection on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the objection.

If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

If the corresponding date falls on a weekend or a public holiday, you will have until the next working day to respond.

This means that the exact number of days you have to comply with an objection varies, depending on the month in which it was made.

Example

An organisation receives an objection on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the objection.

If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.

For practical purposes, if a consistent number of days is required (eg for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar

month.

Can we extend the time for a response?

You can extend the time to respond to an objection by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their objection and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- you are requesting proof of identity before considering the request.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the objection you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality. You should take into account what data you hold, the nature of the data, and what you are using it for.

You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their objection. The period for responding to the objection begins when you receive the additional information.

Further Reading

 [Relevant provisions in the GDPR - See Articles 6, 12, 21, 89 and Recitals 69 and 70](#) 

External link

Rights related to automated decision making including profiling

At a glance

- The GDPR has provisions on:
 - automated individual decision-making (making a decision solely by automated means without any human involvement); and
 - profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.
- The GDPR applies to all automated individual decision-making and profiling.
- Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.
- You can only carry out this type of decision-making where the decision is:
 - necessary for the entry into or performance of a contract; or
 - authorised by Union or Member state law applicable to the controller; or
 - based on the individual's explicit consent.
- You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:
 - give individuals information about the processing;
 - introduce simple ways for them to request human intervention or challenge a decision;
 - carry out regular checks to make sure that your systems are working as intended.

Checklists

All automated individual decision-making and profiling

To comply with the GDPR...

- We have a lawful basis to carry out profiling and/or automated decision-making and document this in our data protection policy.
- We send individuals a link to our privacy statement when we have obtained their personal data indirectly.
- We explain how people can access details of the information we used to create their profile.
- We tell people who provide us with their personal data how they can object to profiling, including profiling for marketing purposes.
- We have procedures for customers to access the personal data input into the profiles so they

can review and edit for any accuracy issues.

- We have additional checks in place for our profiling/automated decision-making systems to protect any vulnerable groups (including children).
- We only collect the minimum amount of data needed and have a clear retention policy for the profiles we create.

As a model of best practice...

- We carry out a DPIA to consider and address the risks before we start any new automated decision-making or profiling.
- We tell our customers about the profiling and automated decision-making we carry out, what information we use to create the profiles and where we get this information from.
- We use anonymised data in our profiling activities.

Solely automated individual decision-making, including profiling with legal or similarly significant effects (Article 22)

To comply with the GDPR...

- We carry out a DPIA to identify the risks to individuals, show how we are going to deal with them and what measures we have in place to meet GDPR requirements.
- We carry out processing under Article 22(1) for contractual purposes and we can demonstrate why it's necessary.

OR

- We carry out processing under Article 22(1) because we have the individual's explicit consent recorded. We can show when and how we obtained consent. We tell individuals how they can withdraw consent and have a simple way for them to do this.

OR

- We carry out processing under Article 22(1) because we are authorised or required to do so. This is the most appropriate way to achieve our aims.
- We don't use special category data in our automated decision-making systems unless we have a lawful basis to do so, and we can demonstrate what that basis is. We delete any special category data accidentally created.
- We explain that we use automated decision-making processes, including profiling. We explain what information we use, why we use it and what the effects might be.
- We have a simple way for people to ask us to reconsider an automated decision.
- We have identified staff in our organisation who are authorised to carry out reviews and change decisions.

We regularly check our systems for accuracy and bias and feed any changes back into the design process.

As a model of best practice...

We use visuals to explain what information we collect/use and why this is relevant to the process.

We have signed up to [standard] a set of ethical principles to build trust with our customers. This is available on our website and on paper.

In brief

- [What's new under the GDPR?](#)
- [What is automated individual decision-making and profiling?](#)
- [What does the GDPR say about automated individual decision-making and profiling?](#)
- [When can we carry out this type of processing?](#)
- [What else do we need to consider?](#)
- [What if Article 22 doesn't apply to our processing?](#)

What's new under the GDPR?

- Profiling is now specifically defined in the GDPR.
- Solely automated individual decision-making, including profiling with legal or similarly significant effects is restricted.
- There are three grounds for this type of processing that lift the restriction.
- Where one of these grounds applies, you must introduce additional safeguards to protect data subjects. These work in a similar way to existing rights under the 1998 Data Protection Act.
- The GDPR requires you to give individuals specific information about automated individual decision-making, including profiling.
- There are additional restrictions on using special category and children's personal data.

What is automated individual decision-making and profiling?

Automated individual decision-making is a decision made by automated means without any human involvement.

Examples of this include:

- an online decision to award a loan; and
- a recruitment aptitude test which uses pre-programmed algorithms and criteria.

Automated individual decision-making does not have to involve profiling, although it often will do.

The GDPR says that profiling is:



“Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”

[Article 4(4)]

Organisations obtain personal information about individuals from a variety of different sources. Internet searches, buying habits, lifestyle and behaviour data gathered from mobile phones, social networks, video surveillance systems and the Internet of Things are examples of the types of data organisations might collect.

Information is analysed to classify people into different groups or sectors, using algorithms and machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals. There is more information about algorithms and machine-learning in our paper on [big data, artificial intelligence, machine learning and data protection](#).

Based on the traits of others who appear similar, organisations use profiling to:

- find something out about individuals’ preferences;
- predict their behaviour; and/or
- make decisions about them.

This can be very useful for organisations and individuals in many sectors, including healthcare, education, financial services and marketing.

Automated individual decision-making and profiling can lead to quicker and more consistent decisions. But if they are used irresponsibly there are significant risks for individuals. The GDPR provisions are designed to address these risks.

What does the GDPR say about automated individual decision-making and profiling?

The GDPR restricts you from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.



“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

[Article 22(1)]

For something to be solely automated there must be no human involvement in the decision-making process.

The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision.

A legal effect is something that adversely affects someone's legal rights. Similarly significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

When can we carry out this type of processing?

Solely automated individual decision-making - including profiling - with legal or similarly significant effects is restricted, although this restriction can be lifted in certain circumstances.

You can **only** carry out solely automated decision-making with legal or similarly significant effects if the decision is:

- necessary for entering into or performance of a contract between an organisation and the individual;
- authorised by law (for example, for the purposes of fraud or tax evasion); or
- based on the individual's explicit consent.

If you're using special category personal data you can **only** carry out processing described in Article 22(1) if:

- you have the individual's explicit consent; **or**
- the processing is necessary for reasons of substantial public interest.

What else do we need to consider?

Because this type of processing is considered to be high-risk the GDPR requires you to carry out a Data Protection Impact Assessment (DPIA) to show that you have identified and assessed what those risks are and how you will address them.

As well as restricting the circumstances in which you can carry out solely automated individual decision-making (as described in Article 22(1)) the GDPR also:

- requires you to give individuals specific information about the processing;
- obliges you to take steps to prevent errors, bias and discrimination; and
- gives individuals rights to challenge and request a review of the decision.

These provisions are designed to increase individuals' understanding of how you might be using their personal data.

You must:

- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;
- use appropriate mathematical or statistical procedures;
- ensure that individuals can:
 - obtain human intervention;

- express their point of view; and
- obtain an explanation of the decision and challenge it;
- put appropriate technical and organisational measures in place, so that you can correct inaccuracies and minimise the risk of errors;
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects.

What if Article 22 doesn't apply to our processing?

Article 22 applies to solely automated individual decision-making, including profiling, with legal or similarly significant effects.

If your processing does not match this definition then you can continue to carry out profiling and automated decision-making.

But you must still comply with the GDPR principles.

You must identify and record your [lawful basis for the processing](#).

You need to have processes in place so people can [exercise their rights](#).

Individuals have a right to object to profiling in certain circumstances. You must bring details of this right specifically to their attention.

Further Reading

 [Relevant provisions in the GDPR - Article 4\(4\), 9, 12, 13, 14, 15, 21, 22, 35\(1\) and \(3\)](#) 
External link

In more detail – ICO guidance

We have published detailed guidance on [automated decision-making and profiling](#).

[Privacy notices transparency and control](#)

[Big data, artificial intelligence, machine learning and data protection](#)

In more detail – Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

Following the consultation period, the Article 29 Working Party has adopted final [guidelines on Automated individual decision-making and Profiling](#).

Other relevant guidelines published by WP29 include:

Accountability and governance

At a glance

- Accountability is one of the data protection principles - it makes you responsible for complying with the GDPR and says that you must be able to demonstrate your compliance.
- You need to put in place appropriate technical and organisational measures to meet the requirements of accountability.
- There are a number of measures that you can, and in some cases must, take including:
 - adopting and implementing data protection policies;
 - taking a 'data protection by design and default' approach;
 - putting written contracts in place with organisations that process personal data on your behalf;
 - maintaining documentation of your processing activities;
 - implementing appropriate security measures;
 - recording and, where necessary, reporting personal data breaches;
 - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
 - appointing a data protection officer; and
 - adhering to relevant codes of conduct and signing up to certification schemes.
- Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.
- If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.
- Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.

Checklist

We take responsibility for complying with the GDPR, at the highest management level and throughout our organisation.

We keep evidence of the steps we take to comply with the GDPR.

We put in place appropriate technical and organisational measures, such as:

adopting and implementing data protection policies (where proportionate);

taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;

putting written contracts in place with organisations that process personal data on our behalf;

- maintaining documentation of our processing activities;
 - implementing appropriate security measures;
 - recording and, where necessary, reporting personal data breaches;
 - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
 - appointing a data protection officer (where necessary); and
 - adhering to relevant codes of conduct and signing up to certification schemes (where possible).
- We review and update our accountability measures at appropriate intervals.

In brief

- [What's new under the GDPR?](#)
- [What is accountability?](#)
- [Why is accountability important?](#)
- [What do we need to do?](#)
- [Should we implement data protection policies?](#)
- [Should we adopt a 'data protection by design and default' approach?](#)
- [Do we need to use contracts?](#)
- [What documentation should we maintain?](#)
- [What security measures should we put in place?](#)
- [How do we record and report personal data breaches?](#)
- [Should we carry out data protection impact assessments \(DPIAs\)?](#)
- [Should we assign a data protection officer \(DPO\)?](#)
- [Should we adhere to codes of conduct and certification schemes?](#)
- [What else should we consider?](#)

What's new under the GDPR?

One of the biggest changes introduced by the GDPR is around accountability – a new data protection principle that says organisations are responsible for, and must be able to demonstrate, compliance with the other principles. Although these obligations were implicit in the Data Protection Act 1998 (1998 Act), the GDPR makes them explicit.

You now need to be proactive about data protection, and evidence the steps you take to meet your obligations and protect people's rights. Good practice tools that the ICO has championed for a long time, such as privacy impact assessments and privacy by design, are now formally recognised and legally required in some circumstances.

Organisations that already adopt a best practice approach to compliance with the 1998 Act should not find it too difficult to adapt to the new requirements. But you should review the measures you take to comply with the 1998 Act, update them for the GDPR if necessary, and stand ready to demonstrate your compliance under the GDPR.

Further Reading

 [Relevant provisions in the GDPR - See Articles 5 and 24, and Recitals 39 and 74](#) 
External link

What is accountability?

There are two key elements. First, the accountability principle makes it clear that you are **responsible** for complying with the GDPR. Second, you must be able to **demonstrate** your compliance.

Article 5(2) of the GDPR says:



“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the other data protection principles]”

Further Reading

 [Relevant provisions in the GDPR - See Article 5 and Recital 39](#) 
External link

Further reading – ICO guidance

[Principles](#)

Why is accountability important?

Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people’s rights not only results in better legal compliance, it also offers you a competitive edge. Accountability is a real opportunity for you to show, and prove, how you respect people’s privacy. This can help you to develop and sustain people’s trust.

Furthermore, if something does go wrong, then being able to show that you actively considered the risks and put in place measures and safeguards can help you provide mitigation against any potential enforcement action. On the other hand, if you can’t show good data protection practices, it may leave you open to fines and reputational damage.

Further Reading

What do we need to do?

Accountability is not a box-ticking exercise. Being **responsible** for compliance with the GDPR means that you need to be proactive and organised about your approach to data protection, while **demonstrating** your compliance means that you must be able to evidence the steps you take to comply.

To achieve this, if you are a larger organisation you may choose to put in place a privacy management framework. This can help you create a culture of commitment to data protection, by embedding systematic and demonstrable compliance across your organisation. Amongst other things, your framework should include:

- robust program controls informed by the requirements of the GDPR;
- appropriate reporting structures; and
- assessment and evaluation procedures.

If you are a smaller organisation you will most likely benefit from a smaller scale approach to accountability. Amongst other things you should:

- ensure a good level of understanding and awareness of data protection amongst your staff;
- implement comprehensive but proportionate policies and procedures for handling personal data; and
- keep records of what you do and why.

Article 24(1) of the GDPR says that:

- you must implement technical and organisational measures to ensure, and demonstrate, compliance with the GDPR;
- the measures should be risk-based and proportionate; and
- you need to review and update the measures as necessary.

While the GDPR does not specify an exhaustive list of things you need to do to be accountable, it does set out several different measures you can take that will help you get there. These are summarised under the headings below, with links to the relevant parts of the guide. Some measures you are obliged to take and some are voluntary. It will differ depending on what personal data you have and what you do with it. These measures can form the basis of your programme controls if you opt to put in place a privacy management framework across your organisation.

Should we implement data protection policies?

For many organisations, putting in place relevant policies is a fundamental part of their approach to data protection compliance. The GDPR explicitly says that, where proportionate, implementing data protection policies is one of the measures you can take to ensure, and demonstrate, compliance.

What you have policies for, and their level of detail, depends on what you do with personal data. If, for

instance, you handle large volumes of personal data, or particularly sensitive information such as special category data, then you should take greater care to ensure that your policies are robust and comprehensive.

As well as drafting data protection policies, you should also be able to show that you have implemented and adhered to them. This could include awareness raising, training, monitoring and audits – all tasks that your data protection officer can undertake ([see below for more on data protection officers](#)).

Further Reading

 [Relevant provisions in the GDPR - See Articles 24\(2\) and Recital 78](#) 

External link

Should we adopt a ‘data protection by design and default’ approach?

Privacy by design has long been seen as a good practice approach when designing new products, processes and systems that use personal data. Under the heading ‘data protection by design and by default’, the GDPR legally requires you to take this approach.

Data protection by design and default is an integral element of being accountable. It is about embedding data protection into everything you do, throughout all your processing operations. The GDPR suggests measures that may be appropriate such as minimising the data you collect, applying pseudonymisation techniques, and improving security features.

Integrating data protection considerations into your operations helps you to comply with your obligations, while documenting the decisions you take (often in [data protection impact assessments – see below](#)) demonstrates this.

Further Reading

 [Relevant provisions in the GDPR - See Article 25 and Recital 78](#) 

External link

Further reading – ICO guidance

[Data protection by design and default](#)

[Anonymisation](#) code of practice

Do we need to use contracts?

Whenever a controller uses a processor to handle personal data on their behalf, it needs to put in place a written contract that sets out each party’s responsibilities and liabilities.

Contracts must include certain specific terms as a minimum, such as requiring the processor to take appropriate measures to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the GDPR.

Using clear and comprehensive contracts with your processors helps to ensure that everyone understands their data protection obligations and is a good way to demonstrate this formally.

Further Reading

 [Relevant provisions in the GDPR - See Article 28 and Recital 81](#) 

External link

Further reading – ICO guidance

[Contracts](#)

What documentation should we maintain?

Under Article 30 of the GDPR, most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention.

Documenting this information is a great way to take stock of what you do with personal data. Knowing what information you have, where it is and what you do with it makes it much easier for you to comply with other aspects of the GDPR such as making sure that the information you hold about people is accurate and secure.

As well as your record of processing activities under Article 30, you also need to document other things to show your compliance with the GDPR. For instance, you need to keep records of consent and any personal data breaches.

Further Reading

 [Relevant provisions in the GDPR - See Articles 7\(1\), 30 and 33\(5\), and Recitals 42 and 82](#) 

External link

Further reading – ICO guidance

[Documentation](#)

[Consent](#)

[Personal data breaches](#)

What security measures should we put in place?

The GDPR repeats the requirement to implement technical and organisational measures to comply with the GDPR in the context of security. It says that these measures should ensure a level of security appropriate to the risk.

You need to implement security measures if you are handling any type of personal data, but what you put in place depends on your particular circumstances. You need to ensure the confidentiality, integrity and availability of the systems and services you use to process personal data.

Amongst other things, this may include information security policies, access controls, security monitoring, and recovery plans.

Further Reading

 [Relevant provisions in the GDPR - See Articles 5\(f\) and 32, and Recitals 39 and 83](#) 
External link

Further reading – ICO guidance

[Security](#)

How do we record and report personal data breaches?

You must report certain types of personal data breach to the relevant supervisory authority (for the UK, this is the ICO), and in some circumstances, to the affected individuals as well.

Additionally, the GDPR says that you must keep a record of any personal data breaches, regardless of whether you need to report them or not.

You need to be able to detect, investigate, report (both internally and externally) and document any breaches. Having robust policies, procedures and reporting structures helps you do this.

Further Reading

 [Relevant provisions in the GDPR - See Articles 33-34 and Recitals 85-88](#) 
External link

Further reading – ICO guidance

[Personal data breaches](#)

Further reading – Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

[WP29 guidelines on Personal data breach notification](#)

Should we carry out data protection impact assessments (DPIAs)?

A DPIA is an essential accountability tool and a key part of taking a data protection by design approach to what you do. It helps you to identify and minimise the data protection risks of any new projects you undertake.

A DPIA is a legal requirement before carrying out processing likely to result in high risk to individuals' interests.

When done properly, a DPIA helps you assess how to comply with the requirements of the GDPR, while also acting as documented evidence of your decision-making and the steps you took.

Further Reading

 [Relevant provisions in the GDPR - See Articles 35-36, and Recitals 84 and 89-95](#) 

External link

Further reading – ICO guidance

[Data protection impact assessments](#)

Further reading – Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

[WP29 guidelines on Data Protection Impact Assessments](#)

Should we assign a data protection officer (DPO)?

Some organisations are required to appoint a DPO. A DPO's tasks include advising you about the GDPR, monitoring compliance and training staff.

Your DPO must report to your highest level of management, operate independently, and have adequate resources to carry out their tasks.

Even if you're not obliged to appoint a DPO, it is very important that you have sufficient staff, skills, and appropriate reporting structures in place to meet your obligations under the GDPR.

Further Reading

 [Relevant provisions in the GDPR - See Articles 37-39, and Recital 97](#) 

External link

Further reading – ICO guidance

[Data protection officers](#)

Further reading – Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

[WP29 guidelines on Data Protection Officers](#)

Should we adhere to codes of conduct and certification schemes?

Under the GDPR, trade associations and representative bodies may draw up codes of conduct covering topics such as fair and transparent processing, pseudonymisation, and the exercise of people's rights.

In addition, supervisory authorities or accredited certification bodies can issue certification of the data protection compliance of products and services.

Both codes of conduct and certification are voluntary, but they are an excellent way of verifying and demonstrating that you comply with the GDPR.

Further Reading

 [Relevant provisions in the GDPR - See Articles 40-43, and Recitals 98 and 100](#) 
External link

Further reading – ICO guidance

[Codes of conduct and certification](#)

What else should we consider?

The above measures can help to support an accountable approach to data protection, but it is not limited to these. You need to be able to prove what steps you have taken to comply. In practice this means keeping records of what you do and justifying your decisions.

Example

A company wants to use the personal data it holds for a new purpose. It carries out an assessment

in line with Article 6(4) of the GDPR, and determines that the new purpose is compatible with the original purpose for which it collected the personal data. Although this provision of the GDPR does not specify that the company must document its compatibility assessment, it knows that to be accountable, it needs to be able to prove that their handling of personal data is compliant with the GDPR. The company therefore keeps a record of the compatibility assessment, including its rationale for the decision and the appropriate safeguards it put in place.

Accountability is not just about being answerable to the regulator; you must also demonstrate your compliance to individuals. Amongst other things, individuals have the right to be informed about what personal data you collect, why you use it and who you share it with. Additionally, if you use techniques such as artificial intelligence and machine learning to make decisions about people, in certain cases individuals have the right to hold you to account by requesting explanations of those decisions and contesting them. You therefore need to find effective ways to provide information to people about what you do with their personal data, and explain and review automated decisions.

The obligations that accountability places on you are ongoing – you cannot simply sign off a particular processing operation as ‘accountable’ and move on. You must review the measures you implement at appropriate intervals to ensure that they remain effective. You should update measures that are no longer fit for purpose. If you regularly change what you do with personal data, or the types of information that you collect, you should review and update your measures frequently, remembering to document what you do and why.

Further Reading

 [Relevant provisions in the GDPR - See Articles 12-14, 22 and 24\(1\), and Recitals 39, 58-61 and 71](#)



External link

Further reading – ICO guidance

[Right to be informed](#)

[Rights related to automated decision making including profiling](#)

[Data protection self assessment](#)

Contracts

At a glance

- Whenever a controller uses a processor it needs to have a written contract in place.
- The contract is important so that both parties understand their responsibilities and liabilities.
- The GDPR sets out what needs to be included in the contract.
- In the future, standard contract clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However at the moment no standard clauses have been drafted.
- Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement – though again, no such schemes are currently available.
- Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

Checklists

Controller and processor contracts checklist

Our contracts include the following compulsory details:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

Our contracts include the following compulsory terms:

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;

- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

As a matter of good practice, our contracts:

- state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and
- reflect any indemnity that has been agreed.

Processors' responsibilities and liabilities checklist

In addition to the Article 28.3 contractual obligations set out in the controller and processor contracts checklist, a processor has the following direct responsibilities under the GDPR. The processor must:

- only act on the written instructions of the controller (Article 29);
- not use a sub-processor without the prior written authorisation of the controller (Article 28.2);
- co-operate with supervisory authorities (such as the ICO) in accordance with Article 31;
- ensure the security of its processing in accordance with Article 32;
- keep records of its processing activities in accordance with Article 30.2;
- notify any personal data breaches to the controller in accordance with Article 33;
- employ a data protection officer if required in accordance with Article 37; and
- appoint (in writing) a representative within the European Union if required in accordance with Article 27.

A processor should also be aware that:

- it may be subject to investigative and corrective powers of supervisory authorities (such as the ICO) under Article 58 of the GDPR;
- if it fails to meet its obligations, it may be subject to an administrative fine under Article 83 of the GDPR;
- if it fails to meet its GDPR obligations it may be subject to a penalty under Article 84 of the GDPR; and
- if it fails to meet its GDPR obligations it may have to pay compensation under Article 82 of the GDPR.

In brief

What's new?

- The GDPR makes written contracts between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA.
- These contracts must now include certain specific terms, as a minimum.
- These terms are designed to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).
- The GDPR allows for standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) to be used in contracts between controllers and processors - though none have been drafted so far.

- The GDPR envisages that adherence by a processor to an approved code of conduct or certification scheme may be used to help controllers demonstrate that they have chosen a suitable processor. Standard contractual clauses may form part of such a code or scheme, though again, no schemes are currently available.
- The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.

When is a contract needed?

Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place. Similarly, if a processor employs another processor it needs to have a written contract in place.

Why are contracts between controllers and processors important?

Contracts between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. They help them to comply with the GDPR, and help controllers to demonstrate their compliance with the GDPR. The use of contracts by controllers and processors may also increase data subjects' confidence in the handling of their personal data.

What needs to be included in the contract?

Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Can standard contracts clauses be used?

The GDPR allows standard contractual clauses from the EU Commission or a Supervisory Authority (such as the ICO) to be used in contracts between controllers and processors. However, no standard clauses are currently available.

The GDPR also allows these standard contractual clauses to form part of a code of conduct or certification mechanism to demonstrate compliant processing. However, no schemes are currently available.

What responsibilities and liabilities do processors have in their own right?

A processor must only act on the documented instructions of a controller. If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

In addition to its contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:

- not to use a sub-processor without the prior written authorisation of the data controller;
- to co-operate with supervisory authorities (such as the ICO);
- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer; and
- to appoint (in writing) a representative within the European Union if needed.

If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

Further Reading

 [Relevant provisions in the GDPR - see Articles 28-36 and Recitals 81-83](#) 

External link

In more detail – ICO guidance

The deadline for responses to our [draft GDPR guidance on contracts and liabilities for controllers and processors](#) has now passed. We are analysing the feedback and this will feed into the final version.

Documentation

At a glance

- The GDPR contains explicit provisions about documenting your processing activities.
- You must maintain records on several things such as processing purposes, data sharing and retention.
- You may be required to make the records available to the ICO on request.
- Documentation can help you comply with other aspects of the GDPR and improve your data governance.
- Controllers and processors both have documentation obligations.
- For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.
- Information audits or data-mapping exercises can feed into the documentation of your processing activities.
- Records must be kept in writing.
- Most organisations will benefit from maintaining their records electronically.
- Records must be kept up to date and reflect your current processing activities.
- We have produced some basic templates to help you document your processing activities.

Checklists

Documentation of processing activities – requirements

If we are a controller for the personal data we process, we document all the applicable information under Article 30(1) of the GDPR.

If we are a processor for the personal data we process, we document all the applicable information under Article 30(2) of the GDPR.

If we process special category or criminal conviction and offence data, we document:

the condition for processing we rely on in the Data Protection Bill;

the lawful basis for our processing; and

whether we retain and erase the personal data in accordance with our policy document.

We document our processing activities in writing.

We document our processing activities in a granular way with meaningful links between the different pieces of information.

We conduct regular reviews of the personal data we process and update our documentation accordingly.

Documentation of processing activities – best practice

When preparing to document our processing activities we:

- do information audits to find out what personal data our organisation holds;
- distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and
- review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities we document, or link to documentation, on:

- information required for privacy notices;
 - records of consent;
 - controller-processor contracts;
 - the location of personal data;
 - Data Protection Impact Assessment reports; and
 - records of personal data breaches.
- We document our processing activities in electronic form so we can add, remove and amend information easily.

In brief

- [What's new under the GDPR?](#)
- [What is documentation?](#)
- [Who needs to document their processing activities?](#)
- [What do we need to document under Article 30 of the GDPR?](#)
- [Should we document anything else?](#)
- [How do we document our processing activities?](#)

What's new under the GDPR?

- The documentation of processing activities is a new requirement under the GDPR.
- There are some similarities between documentation under the GDPR and the information you provided to the ICO as part of registration under the Data Protection Act 1998.
- You need to make sure that you have in place a record of your processing activities by 25 May 2018.

What is documentation?

- Most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention; we call this **documentation**.
- Documenting your processing activities is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other aspects of the GDPR.

Who needs to document their processing activities?

- Controllers and processors each have their own documentation obligations.
- If you have 250 or more employees, you must document all your processing activities.
- There is a limited exemption for small and medium-sized organisations. If you have fewer than 250 employees, you only need to document processing activities that:
 - are not occasional; or
 - could result in a risk to the rights and freedoms of individuals; or
 - involve the processing of special categories of data or criminal conviction and offence data.

What do we need to document under Article 30 of the GDPR?

You must document the following information:

- The name and contact details of your organisation (and where applicable, of other controllers, your representative and your data protection officer).
- The purposes of your processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of your technical and organisational security measures.

Should we document anything else?

As part of your record of processing activities, it can be useful to document (or link to documentation of) other aspects of your compliance with the GDPR and the UK's Data Protection Bill. Such documentation may include:

- information required for privacy notices, such as:
 - the lawful basis for the processing
 - the legitimate interests for the processing
 - individuals' rights
 - the existence of automated decision-making, including profiling
 - the source of the personal data;
- records of consent;

- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports;
- records of personal data breaches;
- information required for processing special category data or criminal conviction and offence data under the Data Protection Bill, covering:
 - the condition for processing in the Data Protection Bill
 - the lawful basis for the processing in the GDPR
 - your retention and erasure policy document.

How do we document our processing activities?

- Doing an information audit or data-mapping exercise can help you find out what personal data your organisation holds and where it is.
- You can find out why personal data is used, who it is shared with and how long it is kept by distributing questionnaires to relevant areas of your organisation, meeting directly with key business functions, and reviewing policies, procedures, contracts and agreements.
- When documenting your findings, the records you keep must be in writing. The information must be documented in a granular and meaningful way.

We have developed basic templates to help you document your processing activities.

Further Reading

 [Documentation template for controllers](#) 

For organisations
File (34.42K)

 [Documentation template for processors](#) 

For organisations
File (19.48K)

Further Reading

 [Relevant provisions in the GDPR – See Article 30 and Recital 82](#) 

External link

 [Relevant provisions in the Data Protection Bill – See Schedule 1](#) 

External link

In more detail – ICO guidance

We have produced [more detailed guidance on documentation](#).

In more detail - Article 29

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 has published a [position paper on Article 30\(5\)](#) (the exemption for small and medium-sized organisations).

Data protection by design and default

At a glance

- The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'.
- In essence, this means you have to integrate or 'bake in' data protection into your processing activities and business practices, from the design stage right through the lifecycle.
- This concept is not new. Previously known as 'privacy by design', it has always been part of data protection law. The key change with the GDPR is that it is now a legal requirement.
- Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

Checklists

- We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- We make data protection an essential component of the core functionality of our processing systems and services.
- We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
- We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.
- We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.
- We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.
- We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.
- We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.
- We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
- We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

- When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.
- We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

In brief

- [What's new in the GDPR?](#)
- [What does the GDPR say about data protection by design and by default?](#)
- [What is data protection by design?](#)
- [What is data protection by default?](#)
- [Who is responsible for complying with data protection by design and by default?](#)
- [What are we required to do?](#)
- [When should we do this?](#)
- [What are the underlying concepts of data protection by design and by default?](#)
- [How do we do this in practice?](#)
- [How do data protection by design and by default link to data protection impact assessments \(DPIAs\)?](#)
- [What is the role of privacy-enhancing technologies \(PETs\)?](#)
- [What about international transfers?](#)
- [What is the role of certification?](#)
- [What additional guidance is available?](#)

What's new in the GDPR?

The GDPR introduces new obligations that require you to integrate data protection concerns into every aspect of your processing activities. This approach is 'data protection by design and by default'. These are key elements of the GDPR's risk-based approach and its focus on accountability, ie you are able to demonstrate how you are complying with its requirements.

However, data protection by design and by default is not new. It is essentially the GDPR's version of 'privacy by design', an approach that the ICO has championed for many years. Although privacy by design and data protection by design are not precisely the same, there are well-established privacy by design principles and practices that can apply in this context.

Some organisations already adopt a 'privacy by design approach' as a matter of good practice. If this is the case for you, then you are well-placed to meet the requirements of data protection by design and by default. Although you may still need to review your processes and procedures to ensure that you are meeting your obligations.

The biggest change is that whilst privacy by design was good practice under the Data Protection Act 1998 (the 1998 Act), data protection by design and by default are legal requirements under the GDPR.

What does the GDPR say about data protection by design and by default?

Articles 25(1) and 25(2) of the GDPR outline your obligations concerning data protection by design and by default.

Article 25(1) specifies the requirements for data protection by design:



'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'

Article 25(2) specifies the requirements for data protection by default:



'The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.'

Article 25(3) states that if you adhere to an approved certification under Article 42, you can use this as one way of demonstrating your compliance with these requirements.

Further Reading

 [Relevant provisions in the GDPR - Article 25 and Recital 78](#) 

External link

What is data protection by design?

Data protection by design is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

As expressed by the GDPR, it requires you to:

- put in place appropriate technical and organisational measures designed to implement the data

protection principles; and

- integrate safeguards into your processing so that you meet the GDPR's requirements and protect the individual rights.

In essence this means you have to integrate or 'bake in' data protection into your processing activities and business practices.

Data protection by design has broad application. Examples include:

- developing new IT systems, services, products and processes that involve processing personal data;
- developing organisational policies, processes, business practices and/or strategies that have privacy implications;
- physical design;
- embarking on data sharing initiatives; or
- using personal data for new purposes.

The underlying concepts of data protection by design are not new. Under the name 'privacy by design' they have existed for many years. Data protection by design essentially inserts the privacy by design approach into data protection law.

Under the 1998 Act, the ICO supported this approach as it helped you to comply with your data protection obligations. It is now a legal requirement.

What is data protection by default?

Data protection by default requires you to ensure that you only process the data that is necessary to achieve your specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation.

You have to process some personal data to achieve your purpose(s). Data protection by default means you need to specify this data before the processing starts, appropriately inform individuals and only process the data you need for your purpose. It does **not** require you to adopt a 'default to off' solution. What you need to do depends on the circumstances of your processing and the risks posed to individuals.

Nevertheless, you must consider things like:

- adopting a 'privacy-first' approach with any default settings of systems and applications;
- ensuring you do not provide an illusory choice to individuals relating to the data you will process;
- not processing additional data unless the individual decides you can;
- ensuring that personal data is not automatically made publicly available to others unless the individual decides to make it so; and
- providing individuals with sufficient controls and options to exercise their rights.

Who is responsible for complying with data protection by design and by default?

Article 25 specifies that, as the controller, you have responsibility for complying with data protection by design and by default. Depending on your circumstances, you may have different requirements for different areas within your organisation. For example:

- your senior management, eg developing a culture of 'privacy awareness' and ensuring you develop policies and procedures with data protection in mind;
- your software engineers, system architects and application developers, –eg those who design systems, products and services should take account of data protection requirements and assist you in complying with your obligations; and
- your business practices, eg you should ensure that you embed data protection by design in all your internal processes and procedures.

This may not apply to all organisations, of course. However, data protection by design is about adopting an organisation-wide approach to data protection, and 'baking in' privacy considerations into any processing activity you undertake. It doesn't apply only if you are the type of organisation that has your own software developers and systems architects.

In considering whether to impose a penalty, the ICO will take into account the technical and organisational measures you have put in place in respect of data protection by design. Additionally, under the Data Protection Bill we can issue an Enforcement Notice against you for any failings in respect of Article 25.

What about data processors?

If you use another organisation to process personal data on your behalf, then that organisation is a data processor under the GDPR.

Article 25 does not mention data processors specifically. However, Article 28 specifies the considerations you must take whenever you are selecting a processor. For example, you must only use processors that provide:



'sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'

This requirement covers both data protection by design in Article 25 as well as your security obligations under Article 32. Your processor cannot necessarily assist you with your data protection by design obligations (unlike with security measures), however you must only use processors that provide sufficient guarantees to meet the GDPR's requirements.

What about other parties?

Data protection by design and by default can also impact organisations other than controllers and processors. Depending on your processing activity, other parties may be involved, even if this is just where you purchase a product or service that you then use in your processing. Examples include manufacturers, product developers, application developers and service providers.

Recital 78 extends the concepts of data protection by design to other organisations, although it does not place a requirement on them to comply – that remains with you as the controller. It says:



'When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.'

Therefore, when considering what products and services you need for your processing, you should look to choose those where the designers and developers have taken data protection into account. This can help to ensure that your processing adheres to the data protection by design requirements.

If you are a developer or designer of products, services and applications, the GDPR places no specific obligations on you about how you design and build these products. (You may have specific obligations as a controller in your own right, eg for any employee data.) However, you should note that controllers are required to consider data protection by design when selecting services and products for use in their data processing activities – therefore if you design these products with data protection in mind, you may be in a better position.

Further Reading

 [Relevant provisions in the GDPR - Articles 25 and 28, and Recitals 78, 79, 81 and 82](#) 

External link

What are we required to do?

You must put in place appropriate technical and organisational measures designed to implement the data protection principles and safeguard individual rights.

There is no 'one size fits all' method to do this, and no one set of measures that you should put in place. It depends on your circumstances.

The key is that you consider data protection issues from the start of any processing activity, and adopt appropriate policies and measures that meet the requirements of data protection by design and by default.

Some examples of how you can do this include:

- minimising the processing of personal data;
- pseudonymising personal data as soon as possible;
- ensuring transparency in respect of the functions and processing of personal data;
- enabling individuals to monitor the processing; and
- creating (and improving) security features.

This is not an exhaustive list. Complying with data protection by design and by default may require you to do much more than the above.

However, we cannot provide a complete guide to all aspects of data protection by design and by default in all circumstances. This guidance identifies the main points for you to consider. Depending on the processing you are doing, you may need to obtain specialist advice that goes beyond the scope of this guidance.

Further Reading

 [Relevant provisions in the GDPR - Recital 78](#) 

External link

When should we do this?

You should begin data protection by design at the initial phase of any system, service, product, or process. You should start by considering your intended processing activities, the risks that these may pose to individuals, and the possible measures available to ensure that you comply with the data protection principles and protect individual rights. These considerations must cover:

- the state of the art and costs of implementation of any measures;
- the nature, scope, context and purposes of your processing; and
- the risks that your processing poses to the rights and freedoms of individuals.

This is similar to the information risk assessment you should do when considering your security measures.

These considerations lead into the second step, where you put in place actual technical and organisational measures to implement the data protection principles and integrate safeguards into your processing.

This is why there is no single solution or process that applies to every organisation or every processing activity, although there are a number of commonalities that may apply to your specific circumstances as described below.

The GDPR requires you to take these actions:

- 'at the time of the determination of the means of the processing' – in other words, when you are at the design phase of any processing activity; and
- 'at the time of the processing itself' – ie during the lifecycle of your processing activity.

What are the underlying concepts of data protection by design and by default?

The underlying concepts are essentially expressed in the seven 'foundational principles' of privacy by design, as developed by the Information and Privacy Commissioner of Ontario.

Although privacy by design is not necessarily equivalent to data protection by design, these foundational principles can nevertheless underpin any approach you take.

'Proactive not reactive; preventative not remedial'

You should take a proactive approach to data protection and anticipate privacy issues and risks before they happen, instead of waiting until after the fact. This doesn't just apply in the context of systems

design – it involves developing a culture of ‘privacy awareness’ across your organisation.

‘Privacy as the default setting’

You should design any system, service, product, and/or business practice to protect personal data automatically. With privacy built into the system, the individual does not have to take any steps to protect their data – their privacy remains intact without them having to do anything.

‘Privacy embedded into design’

Embed data protection into the design of any systems, services, products and business practices. You should ensure data protection forms part of the core functions of any system or service – essentially, it becomes integral to these systems and services.

‘Full functionality – positive sum, not zero sum’

Also referred to as ‘win-win’, this principle is essentially about avoiding trade-offs, such the belief that in any system or service it is only possible to have privacy **or** security, not privacy **and** security. Instead, you should look to incorporate all legitimate objectives whilst ensuring you comply with your obligations.

‘End-to-end security – full lifecycle protection’

Put in place strong security measures from the beginning, and extend this security throughout the ‘data lifecycle’ – ie process the data securely and then destroy it securely when you no longer need it.

‘Visibility and transparency – keep it open’

Ensure that whatever business practice or technology you use operates according to its premises and objectives, and is independently verifiable. It is also about ensuring visibility and transparency to individuals, such as making sure they know what data you process and for what purpose(s) you process it.

‘Respect for user privacy – keep it user-centric’

Keep the interest of individuals paramount in the design and implementation of any system or service, eg by offering strong privacy defaults, providing individuals with controls, and ensuring appropriate notice is given.

How do we do this in practice?

One means of putting these concepts into practice is to develop a set of practical, actionable guidelines that you can use in your organisation, framed by your assessment of the risks posed and the measures available to you. You could base these upon the seven foundational principles.

However, how you go about doing this depends on your circumstances – who you are, what you are doing, the resources you have available, and the nature of the data you process. You may not need to have a set of documents and organisational controls in place, although in some situations you will be required to have certain documents available concerning your processing.

The key is to take an organisational approach that achieves certain outcomes, such as ensuring that:

- you consider data protection issues as part of the design and implementation of systems, services,
-

products and business practices;

- you make data protection an essential component of the core functionality of your processing systems and services;
- you only process the personal data that you need in relation to your purposes(s), and that you only use the data for those purposes;
- personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy;
- the identity and contact information of those responsible for data protection are available both within your organisation and to individuals;
- you adopt a 'plain language' policy for any public documents so that individuals easily understand what you are doing with their personal data;
- you provide individuals with tools so they can determine how you are using their personal data, and whether you are properly enforcing your policies; and
- you offer offering strong privacy defaults, user-friendly options and controls, and respect user preferences.

Many of these relate to other obligations in the GDPR, such as transparency requirements, documentation, Data Protection Officers and DPIAs. This shows the broad nature of data protection by design and how it applies to all aspects of your processing. Our guidance on these topics will help you when you consider the measures you need to put in place for data protection by design and by default.

In more detail – ICO guidance

Read our sections on [the data protection principles](#), [individual rights](#), [accountability and governance](#), [documentation](#), [data protection impact assessments](#), [data protection officers](#) and [security](#) in the Guide to the GDPR.

In more detail – Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

Article 29 has produced guidelines on [transparency](#), [data protection officers](#), and [data protection impact assessments](#).

Further reading

We will produce further guidance on how you can implement data protection by design soon. However, the Information and Privacy Commissioner of Ontario has published [guidance on how organisations can 'operationalise' privacy by design](#), which may assist you.

How do data protection by design and by default link to data protection impact assessments (DPIAs)?

A DPIA is a tool that you can use to identify and reduce the data protection risks of your processing activities. They can also help you to design more efficient and effective processes for handling personal data.

DPIAs are an integral part of data protection by design and by default. For example, they can determine the type of technical and organisational measures you need in order to ensure your processing complies with the data protection principles.

However, a DPIA is only required in certain circumstances, such as where the processing is likely to result in a risk to rights and freedoms, though it is good practice to undertake a DPIA anyway. In contrast, data protection by design is a broader concept, as it applies organisationally and requires you to take certain considerations even before you decide whether your processing is likely to result in a high risk or not.

In more detail – ICO guidance

Read our [guidance on DPIAs](#) in the Guide to the GDPR.

We have also produced more [detailed guidance on DPIAs](#), including a [template](#) that you can use and a [list of processing operations](#) that we consider require DPIAs to be undertaken.

In more detail – Article 29

Article 29 has produced [guidelines on data protection impact assessments](#).

What is the role of privacy-enhancing technologies (PETs)?

Privacy-enhancing technologies or PETs are technologies that embody fundamental data protection principles by minimising personal data use, maximising data security, and empowering individuals. A useful definition from the European Union Agency for Network and Information Security (ENISA) refers to PETs as:



'software and hardware solutions, ie systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.'

PETs link closely to the concept of privacy by design, and therefore apply to the technical measures you can put in place. They can assist you in complying with the data protection principles and are a means of implementing data protection by design within your organisation on a technical level.

Further reading

We will provide further guidance on PETs in the near future. ENISA has also published [research reports](#) on PETs that may assist you.

What about international transfers?

Data protection by design also applies in the context of international transfers in cases where you intend to transfer personal data overseas to a third country that does not have an adequacy decision.

You need to ensure that, whatever mechanism you use, appropriate safeguards are in place for these transfers. As detailed in Recital 108, these safeguards need to include compliance with data protection by design and by default.

Further Reading

 [Relevant provisions in the GDPR - Article 47 and Recital 108](#) 

External link

In more detail – ICO guidance

Read our guidance on [international transfers](#).

What is the role of certification?

Article 25(3) says that:

“

‘An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.’

This means that an approved certification mechanism, once one is available, can assist you in showing how you are complying with, and implementing, data protection by design and by default.

In more detail – Article 29

Article 29 will be publishing guidelines on certification criteria soon.

What additional guidance is available?

The ICO will publish more detailed guidance about data protection by design and privacy enhancing

technologies soon, as well as how these concepts apply in the context of the Code of Practice on age appropriate design in the Data Protection Bill.

In the meantime, there are a number of publications about the privacy by design approach. We have summarised some of these below.

Further reading

The **Information and Privacy Commissioner of Ontario** (IPC) originated the concept of privacy by design in the 1990s. The IPC has a number of relevant publications about the concept and how you can implement it in your organisation, including:

- the original [seven foundational principles](#) of privacy by design (external link, PDF); and
- a [primer on privacy by design](#), published in 2013 (external link, PDF); and
- guidance on [Operationalizing privacy by design](#), published in 2012 (external link, PDF)

The **European Union Agency for Network and Information Security** (ENISA) has also published research and guidance on privacy by design, including:

- a research report on [privacy and data protection by design](#) (external link);
- a research report on [privacy by design and big data](#) (external link); and
- a subsection on [privacy-enhancing technologies](#) (external link)

The **Norwegian data protection authority** (Datatilsynet) has [produced guidance](#) on how software developers can implement data protection by design and by default.

Data protection impact assessments

[Click here for information about consulting the ICO about your data protection impact assessment.](#)

At a glance

- A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
- You must do a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing. You can use our screening checklists to help you decide when to do a DPIA.
- It is also good practice to do a DPIA for any other major project which requires the processing of personal data.
- Your DPIA must:
 - describe the nature, scope, context and purposes of the processing;
 - assess necessity, proportionality and compliance measures;
 - identify and assess risks to individuals; and
 - identify any additional measures to mitigate those risks.
- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- You should consult your data protection officer (if you have one) and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.
- If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing.
- The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, we may issue a formal warning not to process the data, or ban the processing altogether.

Checklists

DPIA awareness checklist

- We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.
- Our existing policies, processes and procedures include references to DPIA requirements.
- We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.
- We have created and documented a DPIA process.

- We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist

- We always carry out a DPIA if we plan to:
 - Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
 - Process special category data or criminal offence data on a large scale.
 - Systematically monitor a publicly accessible place on a large scale.
 - Use new technologies.
 - Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
 - Carry out profiling on a large scale.
 - Process biometric or genetic data.
 - Combine, compare or match data from multiple sources.
 - Process personal data without providing a privacy notice directly to the individual.
 - Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
 - Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
 - Process personal data which could result in a risk of physical harm in the event of a security breach.
- We consider whether to do a DPIA if we plan to carry out any other:
 - Evaluation or scoring.
 - Automated decision-making with significant effects.
 - Systematic
 - Processing of sensitive data or data of a highly personal nature.
 - Processing on a large scale.
 - Processing of data concerning vulnerable data subjects.
 - Innovative technological or organisational solutions.
 - Processing involving preventing data subjects from exercising a right or using a service or contract.
- We consider carrying out a DPIA in any major project involving the use of personal data.
- If we decide not to carry out a DPIA, we document our reasons.

- We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

DPIA process checklist

- We describe the nature, scope, context and purposes of the processing.
- We ask our data processors to help us understand and document their processing activities and identify any associated risks.
- We consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- We ask for the advice of our data protection officer.
- We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.
- We do an [objective assessment](#) of the likelihood and severity of any risks to individuals' rights and interests.
- We identify measures we can put in place to eliminate or reduce high risks.
- We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- We implement the measures we identified, and integrate them into our project plan.
- We consult the ICO before processing, if we cannot mitigate high risks.
- We keep our DPIAs under review and revisit them when necessary.

In brief

- [What's new under the GDPR?](#)
- [What is a DPIA?](#)
- [When do we need a DPIA?](#)
- [How do we carry out a DPIA?](#)
- [Do we need to consult the ICO?](#)

What's new under the GDPR?

The GDPR introduces a new obligation to do a DPIA before carrying out types of processing likely to result in high risk to individuals' interests. If your DPIA identifies a high risk that you cannot mitigate, you must consult the ICO.

This is a key element of the new focus on accountability and data protection by design.

Some organisations already carry out privacy impact assessments (PIAs) as a matter of good practice.

If so, the concept will be familiar, but you still need to review your processes to make sure they comply with GDPR requirements. DPIAs are now mandatory in some cases, and there are specific legal requirements for content and process.

If you have not already got a PIA process, you need to design a new DPIA process and embed this into your organisation's policies and procedures.

In the run-up to 25 May 2018, you also need to review your existing processing operations and decide whether you need to do a DPIA, or review your PIA, for anything which is likely to be high risk. You do not need to do a DPIA if you have already considered the relevant risks and safeguards in another way, unless there has been a significant change to the nature, scope, context or purposes of the processing since that previous assessment.

What is a DPIA?

A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It's important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise and you should see it as an ongoing process, and regularly review it.

When do we need a DPIA?

You must do a DPIA before you begin any type of processing which is "likely to result in a high risk". This means that although you have not yet assessed the actual level of risk you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires you to do a DPIA if you plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

You should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data. You can use or adapt the checklists to help you carry out this screening exercise.

How do we carry out a DPIA?

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



You must seek the advice of your data protection officer (if you have one). You should also consult with individuals and other stakeholders throughout this process.

The process is designed to be flexible and scalable. You can use or adapt our [sample DPIA template](#), or create your own. If you want to create your own, you may want to refer to the European guidelines which set out [Criteria for an acceptable DPIA](#).

Although publishing a DPIA is not a requirement of GDPR, you should actively consider the benefits of publication. As well as demonstrating compliance, publication can help engender trust and confidence. We would therefore recommend that you publish your DPIAs, were possible, removing sensitive details if necessary.

Do we need to consult the ICO?

You don't need to send every DPIA to the ICO and we expect the percentage sent to us to be small. But you must consult the ICO if your DPIA identifies a high risk and you cannot take measures to reduce that risk. You cannot begin the processing until you have consulted us.

If you want your project to proceed effectively then investing time in producing a comprehensive DPIA may prevent any delays later, if you have to consult with the ICO.

You need to [email us](#) and attach a copy of your DPIA.

Once we have the information we need, we will generally respond within eight weeks (although we can extend this by a further six weeks in complex cases).

We will provide you with a written response advising you whether the risks are acceptable, or whether you need to take further action. In some cases we may advise you not to carry out the processing because we consider it would be in breach of the GDPR. In appropriate cases we may issue a formal warning or take action to ban the processing altogether.

Further Reading

 [Key provisions in the GDPR - See Articles 35 and 36 and Recitals 74-77, 84, 89-92, 94 and 95](#) 
External link

Further reading – ICO guidance

We have published [more detailed guidance on DPIAs](#).

Further reading – Article 29 guidelines

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The working party has published [Guidelines on Data Protection Impact Assessment \(DPIA\) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 \(WP248\)](#).

Other relevant guidelines include:

[Guidelines on Data Protection Officers \('DPOs'\) \(WP243\)](#)

[Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 \(WP251\)](#)

Data protection officers

At a glance

- The GDPR introduces a duty for you to appoint a data protection officer (DPO) if you are a public authority, or if you carry out certain types of processing activities.
- DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- A DPO can be an existing employee or externally appointed.
- In some cases several organisations can appoint a single DPO between them.
- DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability.

Checklists

Appointing a DPO

- We are a public authority and have appointed a DPO (except if we are a court acting in our judicial capacity).
- We are not a public authority, but we know whether the nature of our processing activities requires the appointment of a DPO.
- We have appointed a DPO based on their professional qualities and expert knowledge of data protection law and practices.
- We aren't required to appoint a DPO under the GDPR but we have decided to do so voluntarily. We understand that the same duties and responsibilities apply had we been required to appoint a DPO. We support our DPO to the same standards.

Position of the DPO

- Our DPO reports directly to our highest level of management and is given the required independence to perform their tasks.
- We involve our DPO, in a timely manner, in all issues relating to the protection of personal data.
- Our DPO is sufficiently well resourced to be able to perform their tasks.
- We do not penalise the DPO for performing their duties.
- We ensure that any other tasks or duties we assign our DPO do not result in a conflict of interests with their role as a DPO.

Tasks of the DPO

- Our DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.
- We will take account of our DPO's advice and the information they provide on our data protection obligations.
- When carrying out a DPIA, we seek the advice of our DPO who also monitors the process.
- Our DPO acts as a contact point for the ICO. They co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter.
- When performing their tasks, our DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Accessibility of the DPO

- Our DPO is easily accessible as a point of contact for our employees, individuals and the ICO.
- We have published the contact details of the DPO and communicated them to the ICO.

In brief

Do we need to appoint a Data Protection Officer?

Under the GDPR, you **must** appoint a DPO if:

- you are a public authority (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

This applies to both controllers and processors. You can appoint a DPO if you wish, even if you aren't required to. If you decide to voluntarily appoint a DPO you should be aware that the same requirements of the position and tasks apply had the appointment been mandatory.

Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and resources to discharge your obligations under the GDPR. However, a DPO can help you operate within the law by advising and helping to monitor compliance. In this way, a DPO can be seen to play a key role in your organisation's data protection governance structure and to help improve accountability.

If you decide that you don't need to appoint a DPO, either voluntarily or because you don't meet the above criteria, it's a good idea to record this decision to help demonstrate compliance with the accountability principle.

What is the definition of a public authority?

The Data Protection Bill will define what a 'public authority' is under GDPR. This is likely to be the same as those defined under the Freedom of Information Act 2000 (FOIA) or the Freedom of Information Act (Scotland) 2002.

This means that if you are already defined as a public authority or public body under FOIA or the Scottish FOIA, it's likely you will be a public authority under the GDPR. However, the Data Protection Bill is subject to amendment and so you should confirm your status when the Bill becomes an Act of Parliament.

What are 'core activities'?

The other two conditions that require you to appoint a DPO only apply when:

- your core activities consist of processing activities, which, by virtue of their nature, scope and / or their purposes, require the regular and systematic monitoring of individuals on a large scale; or
- your core activities consist of processing on a large scale of special category data, or data relating to criminal convictions and offences.

Your core activities are the primary business activities of your organisation. So, if you need to process personal data to achieve your key objectives, this is a core activity. This is different to processing personal data for other secondary purposes, which may be something you do all the time (eg payroll or HR information), but which is not part of carrying out your primary objectives.

Example

For most organisations, processing personal data for HR purposes will be a secondary function to their main business activities and so will not be part of their core activities.

However, a HR service provider necessarily processes personal data as part of its core activities to provide HR functions for its client organisations. At the same time, it will also process HR information for its own employees, which will be regarded as an ancillary function and not part of its core activities.

What does 'regular and systematic monitoring of data subjects on a large scale' mean?

There are two key elements to this condition requiring you to appoint a DPO. Although the GDPR does not define 'regular and systematic monitoring' or 'large scale', the Article 29 Working Party has provided some guidance on these terms in its [guidelines on DPOs](#).

'Regular and systematic' monitoring of data subjects includes all forms of tracking and profiling, both online and offline. An example of this is for the purposes of behavioural advertising.

When determining if processing is on a large scale, the guidelines say you should take the following factors into consideration:

- the numbers of data subjects concerned;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the processing activity.

Example

A large retail website uses algorithms to monitor the searches and purchases of its users and, based on this information, it offers recommendations to them. As this takes place continuously and according to predefined criteria, it can be considered as regular and systematic monitoring of data subjects on a large scale.

What does processing special category data and personal data relating to criminal convictions and offences on a large scale mean?

Processing special category data or criminal conviction or offences data carries more risk than other personal data. So when you process this type of data on a large scale you are required to appoint a DPO, who can provide more oversight. Again, the factors relevant to large-scale processing can include:

- the numbers of data subjects;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the activity.

Example

A health insurance company processes a wide range of personal data about a large number of individuals, including medical conditions and other health information. This can be considered as processing special category data on a large scale.

What professional qualities should the DPO have?

- The GDPR says that you should appoint a DPO on the basis of their professional qualities, and in particular, experience and expert knowledge of data protection law.
- It doesn't specify the precise credentials they are expected to have, but it does say that this should be proportionate to the type of processing you carry out, taking into consideration the level of

protection the personal data requires.

- So, where the processing of personal data is particularly complex or risky, the knowledge and abilities of the DPO should be correspondingly advanced enough to provide effective oversight.
- It would be an advantage for your DPO to also have a good knowledge of your industry or sector, as well as your data protection needs and processing activities.

What are the tasks of the DPO?

The DPO's tasks are defined in Article 39 as:

- to inform and advise you and your employees about your obligations to comply with the GDPR and other data protection laws;
- to monitor compliance with the GDPR and other data protection laws, and with your data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, [data protection impact assessments](#);
- to cooperate with the supervisory authority; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

It's important to remember that the DPO's tasks cover all personal data processing activities, not just those that require their appointment under Article 37(1).

- When carrying out their tasks the DPO is required to take into account the risk associated with the processing you are undertaking. They must have regard to the nature, scope, context and purposes of the processing.
- The DPO should prioritise and focus on the more risky activities, for example where special category data is being processed, or where the potential impact on individuals could be damaging. Therefore, DPOs should provide risk-based advice to your organisation.
- If you decide not to follow the advice given by your DPO, you should document your reasons to help demonstrate your accountability.

Can we assign other tasks to the DPO?

The GDPR says that you can assign further tasks and duties, so long as they don't result in a conflict of interests with the DPO's primary tasks.

Example

As an example of assigning other tasks, Article 30 requires that organisations must maintain records of processing operations. There is nothing preventing this task being allocated to the DPO.

Basically this means the DPO cannot hold a position within your organisation that leads him or her to determine the purposes and the means of the processing of personal data. At the same time, the DPO

shouldn't be expected to manage competing objectives that could result in data protection taking a secondary role to business interests.

Examples

A company's head of marketing plans an advertising campaign, including which of the company's customers to target, what method of communication and the personal details to use. This person cannot also be the company's DPO, as the decision-making is likely to lead to a conflict of interests between the campaign's aims and the company's data protection obligations.

On the other hand, a public authority could appoint its existing FOI officer / records manager as its DPO. There is no conflict of interests here as these roles are about ensuring information rights compliance, rather than making decisions about the purposes of processing.

Can the DPO be an existing employee?

Yes. As long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests, you can appoint an existing employee as your DPO, rather than you having to create a new post.

Can we contract out the role of the DPO?

You can contract out the role of DPO externally, based on a service contract with an individual or an organisation. It's important to be aware that an externally-appointed DPO should have the same position, tasks and duties as an internally-appointed one.

Can we share a DPO with other organisations?

- You may appoint a single DPO to act for a group of companies or public authorities.
- If your DPO covers several organisations, they must still be able to perform their tasks effectively, taking into account the structure and size of those organisations. This means you should consider if one DPO can realistically cover a large or complex collection of organisations. You need to ensure they have the necessary resources to carry out their role and be supported with a team, if this is appropriate.
- Your DPO must be easily accessible, so their contact details should be readily available to your employees, to the ICO, and people whose personal data you process.

Can we have more than one DPO?

- The GDPR clearly provides that an organisation must appoint a single DPO to carry out the tasks required in Article 39, but this doesn't prevent it appointing other data protection specialists as part of a team to help support the DPO.
- You need to determine the best way to set up your organisation's DPO function and whether this necessitates a data protection team. However, there must be an individual designated as the DPO for

the purposes of the GDPR who meets the requirements set out in Articles 37-39.

- If you have a team, you should clearly set out the roles and responsibilities of its members and how it relates to the DPO.
- If you hire data protection specialists other than a DPO, it's important that they are not referred to as your DPO, which is a specific role with particular requirements under the GDPR.

What do we have to do to support the DPO?

You must ensure that:

- the DPO is involved, closely and in a timely manner, in all data protection matters;
- the DPO reports to the highest management level of your organisation, ie board level;
- the DPO operates independently and is not dismissed or penalised for performing their tasks;
- you provide adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) to enable the DPO to meet their GDPR obligations, and to maintain their expert level of knowledge;
- you give the DPO appropriate access to personal data and processing activities;
- you give the DPO appropriate access to other services within your organisation so that they can receive essential support, input or information;
- you seek the advice of your DPO when carrying out a DPIA; and
- you record the details of your DPO as part of your records of processing activities.

This shows the importance of the DPO to your organisation and that you must provide sufficient support so they can carry out their role independently. Part of this is the requirement for your DPO to report to the highest level of management. This doesn't mean the DPO has to be line managed at this level but they must have direct access to give advice to senior managers who are making decisions about personal data processing.

What details do we have to publish about the DPO?

The GDPR requires you to:

- publish the contact details of your DPO; and
- provide them to the ICO.

This is to enable individuals, your employees and the ICO to contact the DPO as needed. You aren't required to include the name of the DPO when publishing their contact details but you can choose to provide this if you think it's necessary or helpful.

You're also required to provide your DPO's contact details in the following circumstances:

- when consulting the ICO under Article 36 about a DPIA; and
- when providing [privacy information](#) to individuals under Articles 13 and 14.

However, remember you do have to provide your DPO's name if you report a [personal data breach](#) to the ICO and to those individuals affected by it.

Is the DPO responsible for compliance?

The DPO isn't personally liable for data protection compliance. As the controller or processor it remains your responsibility to comply with the GDPR. Nevertheless, the DPO clearly plays a crucial role in helping you to fulfil your organisation's data protection obligations.

Further Reading

 [Relevant provisions in the GDPR - See Articles 35-36, 37-39, 83 and Recital 97](#) 

External link

In more detail - ICO guidance

See the following section of the [Guide to GDPR: Accountability and governance](#)

See our [Guide to freedom of information](#)

In more detail – Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party has [published guidelines on DPOs](#) and [DPO FAQs](#).

Codes of conduct

At a glance

- The GDPR recommends that you use approved codes of conduct to help you to apply the GDPR effectively.
- Codes of conduct will reflect the needs of different processing sectors and micro, small and medium sized enterprises.
- Trade associations or bodies representing a sector can create codes of conduct to help their sector comply with the GDPR in an efficient and cost effective way.
- Signing up to a code of conduct is voluntary. However, if there is an approved code of conduct, relevant to your processing, you may wish to consider signing up. It can also help show compliance to the ICO, the public and in your business to business relationships.

In brief

Codes of conduct help you to apply the GDPR effectively and allow you to demonstrate your compliance.

Who is responsible for codes of conduct?

Trade associations or bodies representing a sector can create codes of conduct, in consultation with relevant stakeholders, including the public where feasible. They can amend or extend existing codes to comply with the GDPR requirements. They have to submit the draft code to us for approval.

We will assess whether a monitoring body is independent and has expertise in the subject matter/sector. Approved bodies will monitor compliance with the code (except for codes covering public authorities) and help ensure that the code is appropriately robust and trustworthy.

We will check that codes covering UK processing include:

- appropriate safeguards;
- set out the monitoring body accreditation criteria;
- accredit monitoring bodies;
- publish approved codes; and
- maintain a public register of all UK codes.

If a code covers more than one EU country, the relevant supervisory authority will submit it to the European Data Protection Board (EDPB), who will submit their opinion on the code to the European Commission. The Commission may decide that a code is valid across all EU countries.

If a code covers personal data transfers to countries outside of the EU, the European Commission can use legislation to give a code general validity within the Union.

What should codes of conduct address?

Codes of conduct should help you comply with the law, and may cover topics such as:

- fair and transparent processing;
- legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymisation of personal data;
- the information provided to individuals and the exercise of individuals' rights;
- the information provided to and the protection of children (including mechanisms for obtaining parental consent);
- technical and organisational measures, including data protection by design and by default and security measures;
- breach notification;
- data transfers outside the EU; or
- dispute resolution procedures.

Codes of conduct can collectively address the specific needs of micro, small and medium enterprises and help them to work together to apply GDPR requirements to the specific issues in their sector. Codes are expected to provide added value for their sector, as they will tailor the GDPR requirements to the sector or area of data processing. They could be a cost effective means to enable compliance with GDPR for a sector and its members.

Why sign up to a code of conduct?

Adhering to a code of conduct shows that you:

- follow the GDPR requirements for data protection; and that
- are addressing the level of risk relevant to your sector and the type of processing you are doing. For example, in a 'high risk' sector, such as processing children's or health data, the code may contain more demanding requirements.

Adhering to a code of conduct can help you to:

- be more transparent and accountable - enabling businesses or individuals to distinguish which processing activities, products, and services meet GDPR data protection requirements and they can trust with their personal data;
- have a competitive advantage;
- create effective safeguards to mitigate the risk around data processing and the rights and freedoms of individuals;
- help with specific data protection areas, such as international transfers;
- improve standards by establishing best practice;
- mitigate against enforcement action; and
- demonstrate that you have appropriate safeguards to transfer data to countries outside the EU.

What are the practical implications for our organisation?

- You can sign up to a code of conduct relevant to your data processing activities or sector. This could be an extension or an amendment to a current code, or be a brand new code.

- When you sign up to a code of conduct, you will need to demonstrate to the code's monitoring body, that you meet the code's requirements. These requirements will reflect your sector and size of organisation.
- Your customers will be able to view your code membership via the code's webpage, the ICO's public register of UK approved codes of conduct and the EDPB's public register for all codes of conduct in the EU.
- Once you are assessed as adhering to the code, your compliance with the code will be monitored on a regular basis. This monitoring provides assurance that the code can be trusted. Your membership can be withdrawn if you no longer meet the requirements of the code, and the monitoring body will notify us of this.
- You can help reduce the risk of a fine by signing up to a code of conduct. This is because adherence to a code of conduct will serve as a mitigating factor when a supervisory authority is considering enforcement action via an administrative fine.
- When contracting work to third parties, you may wish to consider whether they have signed up to a code of conduct, as part of meeting your due diligence requirements under the GDPR.

Further Reading

 [Relevant provisions in the GDPR - See Articles 40-4 and 83 and Recitals 77, 98, 99 and 168](#) 
External link

Article 29 Working Party

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party are drafting guidelines on codes of conduct and monitoring bodies to cover the provisions in Articles 40-1 and on codes of conduct as appropriate safeguards for international transfers of personal data (Article 46(2)(e)).

Certification

At a glance

- Member states, supervisory authorities (such as the ICO), the European Data Protection Board (EDPB) and the Commission will promote certification.
- Certification schemes will be a way to comply with the GDPR and enhance your transparency.
- Certification schemes should reflect the needs of micro, small and medium sized enterprises.
- Certification schemes under GDPR will be approved by the ICO and delivered by approved third party assessors.
- Signing up to a certification scheme is voluntary. However, if there is an approved certification scheme that covers your processing activity, you may wish to consider working towards it. It can help you demonstrate compliance to the regulator, the public and in your business to business relationships.

In brief

Who is responsible for certification?

Member states, supervisory authorities (such as the ICO), the European Data Protection Board (EDPB) and the Commission will promote certification as a means to enhance transparency and compliance with the Regulation.

In the UK the certification framework will involve:

- the ICO publishing accreditation requirements for certification bodies to meet;
- the UK's national accreditation body, UKAS, accrediting certification bodies and maintaining a public register;
- the ICO approving and publishing certification criteria for certification schemes;
- accredited certification bodies (third party assessors) issuing certification; and
- controllers and processors applying for certification and using certifications.

The ICO has no plans to accredit certification bodies or carry out certification at this time, although the GDPR does allow this.

Across EU member states, the EDPB will collate all EU certification schemes in a public register. There is also scope for a European Data Seal.

What is the purpose of certification?

Certification is a way of demonstrating that your processing of personal data complies with the GDPR requirements, in line with the accountability principle. It could help you demonstrate to the ICO that you have a systematic and comprehensive approach to compliance. Certification can also help demonstrate data protection in a practical way to businesses, individuals and regulators. Your customers can use certification as a means to quickly assess the level of data protection of your particular product or

service.

The GDPR says that certification is also a means to:

- demonstrate compliance with the provisions on data protection by design and by default (Article 25(3));
- demonstrate that you have appropriate technical and organisational measures to ensure data security (Article 32 (3)); and
- to support transfers of personal data to third countries or international organisations (Article 46(2)(f)).

Why should we apply for certification of our processing?

Applying for certification is voluntary. However, if there is an approved certification scheme that covers your processing activity, you may wish to consider working towards it as a way of demonstrating that you comply with the GDPR.

Obtaining certification for your processing can help you to:

- be more transparent and accountable - enabling businesses or individuals to distinguish which processing activities, products and services meet GDPR data protection requirements and they can trust with their personal data;
- have a competitive advantage;
- create effective safeguards to mitigate the risk around data processing and the rights and freedoms of individuals;
- improve standards by establishing best practice;
- help with international transfers; and
- mitigate against enforcement action.

What are the practical implications for us?

- As a controller or processor, you could obtain certification for your processing operations, products and services. Certification bodies will act as independent assessors, providing an external steer and expertise in data protection. You will need to provide them with all the necessary information and access to your processing activities to enable them to conduct the certification procedure.
- Certification is valid for a maximum of three years, subject to periodic reviews. These independent reviews provide assurance that the certification can be trusted. However, certifications can be withdrawn if you no longer meet the requirements of the certification, and the certification body will notify us of this.
- Your customers can view your certification in a public register of certificates issued by certification bodies.
- Certification can help you demonstrate compliance, but does not reduce your data protection responsibilities. Whilst certification will be considered as a mitigating factor when the ICO is considering imposing a fine, non-compliance with a certification scheme can also be a reason for issuing a fine.
- When contracting work to third parties, you may wish to consider whether they hold a GDPR certificate for their processing operations, as part of meeting your due diligence requirements under

the GDPR.

Further Reading

 [Relevant provisions in the GDPR - See Articles 42-43 and 83 and Recitals 81 and 100](#) 

External link

Article 29 Working Party

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party published [draft guidelines on accreditation for certification bodies](#) for consultation (Article 43). The consultation closed on 30 March 2018.

The Article 29 Working Party are also drafting guidelines on certification and identifying certification criteria (Article 42) and on certification as an appropriate safeguard for international transfers of personal data Article 46(2)(f).

Guide to the data protection fee

The Government has announced a new charging structure for data controllers to ensure the continued funding of the Information Commissioner's Office (ICO).

The new structure was laid before Parliament as a Statutory Instrument and will come into effect on 25 May 2018, to coincide with the General Data Protection Regulation.

Until then, [organisations are legally required to pay the current notification fee](#), unless they are exempt.

To help data controllers understand why there's a new funding model and what they'll be required to pay from 25 May 2018, the ICO has produced a Guide to the Data Protection Fee.

The model must still be approved by Parliament before it is finally confirmed. But our guide reflects the draft and is intended to help data controllers prepare for what Government is proposing.

Further Reading

 [The data protection fee - a guide for controllers](#) 

For organisations
PDF (207.19K)

Security

At a glance

- A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.
- Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
- You also have to take into account additional requirements about the security of your processing – and these also apply to data processors.
- You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
- Where appropriate, you should look to use measures such as pseudonymisation and encryption.
- Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.
- The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.

Checklists

- We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place.
- When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.
- Where necessary, we have additional policies and ensure that controls are in place to enforce them.
- We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.
- We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.
- We use encryption and/or pseudonymisation where it is appropriate to do so.
- We understand the requirements of confidentiality, integrity and availability for the personal

data we process.

- We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.
- We ensure that any data processor we use also implements appropriate technical and organisational measures.

In brief

- [What's new?](#)
- [What does the GDPR say about security?](#)
- [Why should we worry about information security?](#)
- [What do we need to protect with our security measures?](#)
- [What level of security is required?](#)
- [What organisational measures do we need to consider?](#)
- [What technical measures do we need to consider?](#)
- [What if we operate in a sector that has its own security requirements?](#)
- [What do we do when a data processor is involved?](#)
- [What are 'confidentiality, integrity, availability' and 'resilience'?](#)
- [What are the requirements for restoring availability and access to personal data?](#)
- [Are we required to ensure our security measures are effective?](#)
- [What about codes of conduct and certification?](#)
- [What about our staff?](#)

What's new?

The GDPR requires you to process personal data securely. This is not a new data protection obligation. It replaces and mirrors the previous requirement to have 'appropriate technical and organisational measures' under the Data Protection Act 1998 (the 1998 Act).

However, the GDPR provides more specifics about what you have to do about the security of your processing and how you should assess your information risk and put appropriate security measures in place. Whilst these are broadly equivalent to what was considered good and best practice under the 1998 Act, they are now a legal requirement.

What does the GDPR say about security?

Article 5(1)(f) of the GDPR concerns the 'integrity and confidentiality' of personal data. It says that personal data shall be:



'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'

You can refer to this as the GDPR's 'security principle'. It concerns the broad concept of **information security**.

This means that you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. You should remember that while information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures.

You need to consider the security principle alongside Article 32 of the GDPR, which provides more specifics on the security of your processing. Article 32(1) states:



'Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk'

Further Reading

 [Relevant provisions in the GDPR - See Articles 5\(1\)\(f\) and 32, and Recitals 39 and 83](#) 
External link

Why should we worry about information security?

Poor information security leaves your systems and services at risk and may cause real harm and distress to individuals – lives may even be endangered in some extreme cases.

Some examples of the harm caused by the loss or abuse of personal data include:

- identity fraud;
- fake credit card transactions;
- targeting of individuals by fraudsters, potentially made more convincing by compromised personal data;
- witnesses put at risk of physical harm or intimidation;
- offenders at risk from vigilantes;

- exposure of the addresses of service personnel, police and prison officers, and those at risk of domestic violence;
- fake applications for tax credits; and
- mortgage fraud.

Although these consequences do not always happen, you should recognise that individuals are still entitled to be protected from less serious kinds of harm, for example embarrassment or inconvenience.

Information security is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other aspects of the GDPR.

The ICO is also required to consider the technical and organisational measures you had in place when considering an administrative fine.

What do our security measures need to protect?

The security principle goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just cybersecurity. This means the security measures you put in place should seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);
- the data you hold is accurate and complete in relation to why you are processing it; and
- the data remains accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

These are known as 'confidentiality, integrity and availability' and under the GDPR, they form part of your obligations.

What level of security is required?

The GDPR does not define the security measures that you should have in place. It requires you to have a level of security that is 'appropriate' to the risks presented by your processing. You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing.

This reflects both the GDPR's risk-based approach, and that there is no 'one size fits all' solution to information security. It means that what's 'appropriate' for you will depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation.

So, before deciding what measures are appropriate, you need to assess your information risk. You should review the personal data you hold and the way you use it in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised. You should also take account of factors such as:

- the nature and extent of your organisation's premises and computer systems;
- the number of staff you have and the extent of their access to personal data; and
- any personal data held or used by a data processor acting on your behalf.

Further Reading

 [Relevant provisions in the GDPR - See See Article 32\(2\) and Recital 83](#) 

External link

We cannot provide a complete guide to all aspects of security in all circumstances for all organisations, but this guidance is intended to identify the main points for you to consider.

What organisational measures do we need to consider?

Carrying out an information risk assessment is one example of an organisational measure, but you will need to take other measures as well. You should aim to build a culture of security awareness within your organisation. You should identify a person with day-to-day responsibility for information security within your organisation and make sure this person has the appropriate resources and authority to do their job effectively.

Example

The Chief Executive of a medium-sized organisation asks the Director of Resources to ensure that appropriate security measures are in place, and that regular reports are made to the board.

The Resources Department takes responsibility for designing and implementing the organisation's security policy, writing procedures for staff to follow, organising staff training, checking whether security measures are actually being adhered to and investigating security incidents.

Clear accountability for security will ensure that you do not overlook these issues, and that your overall security posture does not become flawed or out of date.

Although an information security policy is an example of an appropriate organisational measure, you may not need a 'formal' policy document or an associated set of policies in specific areas. It depends on your size and the amount and nature of the personal data you process, and the way you use that data. However, having a policy does enable you to demonstrate how you are taking steps to comply with the security principle.

Whether or not you have such a policy, you still need to consider security and other related matters such as:

- co-ordination between key people in your organisation (eg the security manager will need to know about commissioning and disposing of any IT equipment);
- access to premises or equipment given to anyone outside your organisation (eg for computer maintenance) and the additional security considerations this will generate;
- business continuity arrangements that identify how you will protect and recover any personal data you hold; and
- periodic checks to ensure that your security measures remain appropriate and up to date.

What technical measures do we need to consider?

Technical measures are sometimes thought of as the protection of personal data held in computers and networks. Whilst these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen or incorrectly disposed of. Technical measures therefore include both physical and computer or IT security.

When considering physical security, you should look at factors such as:

- the quality of doors and locks, and the protection of your premises by such means as alarms, security lighting or CCTV;
- how you control access to your premises, and how visitors are supervised;
- how you dispose of any paper and electronic waste; and
- how you keep IT equipment, particularly mobile devices, secure.

In the IT context, technical measures may sometimes be referred to as 'cybersecurity'. This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. It may therefore be sensible to assume that your systems are vulnerable and take steps to protect them.

When considering cybersecurity, you should look at factors such as:

- system security – the security of your network and information systems, including those which process personal data;
- data security – the security of the data you hold within your systems, eg ensuring appropriate access controls are in place and that data is held securely;
- online security – eg the security of your website and any other online service or application that you use; and
- device security – including policies on Bring-your-own-Device (BYOD) if you offer it.

Depending on the sophistication of your systems, your usage requirements and the technical expertise of your staff, you may need to obtain specialist information security advice that goes beyond the scope of this guidance. However, it's also the case that you may not need a great deal of time and resources to secure your systems and the personal data they process.

Whatever you do, you should remember the following:

- your cybersecurity measures need to be appropriate to the size and use of your network and information systems;
- you should take into account the state of technological development, but you are also able to consider the costs of implementation;
- your security must be appropriate to your business practices. For example, if you offer staff the ability to work from home, you need to put measures in place to ensure that this does not compromise your security; and
- your measures must be appropriate to the nature of the personal data you hold and the harm that might result from any compromise.

A good starting point is to make sure that you're in line with the requirements of Cyber Essentials – a government scheme that includes a set of basic technical controls you can put in place relatively easily.

You should however be aware that you may have to go beyond these requirements, depending on your processing activities. Cyber Essentials is only intended to provide a 'base' set of controls, and won't

address the circumstances of every organisation or the risks posed by every processing operation.

A list of helpful sources of information about cybersecurity is provided below.

Other resources

[The Cyber Essentials scheme](#) 

In more detail – ICO guidance

Under the 1998 Act, the ICO published a number of more detailed guidance pieces on different aspects of IT security. We will be updating each of these to reflect the GDPR's requirements in due course. However, until that time they may still provide you with assistance or things to consider.

- [IT security top tips](#) – for further general information on IT security;
- [IT asset disposal for organisations](#) (pdf) – guidance to help organisations securely dispose of old computers and other IT equipment;
- [A practical guide to IT security – ideal for the small business](#) (pdf);
- [Protecting personal data in online services – learning from the mistakes of others](#) (pdf) – detailed technical guidance on common technical errors the ICO has seen in its casework
- [Bring your own device \(BYOD\)](#) (pdf) – guidance for organisations who want to allow staff to use personal devices to process personal data;
- [Cloud computing](#) (pdf) – guidance covering how security requirements apply to personal data processed in the cloud; and
- [Encryption](#) – advice on the use of encryption to protect personal data.

What if we operate in a sector that has its own security requirements?

Some industries have specific security requirements or require you to adhere to certain frameworks or standards. These may be set collectively, for example by industry bodies or trade associations, or could be set by other regulators. If you operate in these sectors, you need to be aware of their requirements, particularly if specific technical measures are specified.

Although following these requirements will not necessarily equate to compliance with the GDPR's security principle, the ICO will nevertheless consider these carefully in any considerations of regulatory action. It can be the case that they specify certain measures that you should have, and that those measures contribute to your overall security posture.

Example

If you are processing payment card data, you are obliged to comply with the [Payment Card Industry Data Security Standard](#) . The PCI-DSS outlines a number of specific technical and

organisational measures that the payment card industry considers applicable whenever such data is being processed.

Although compliance with the PCI-DSS is not necessarily equivalent to compliance with the GDPR's security principle, if you process card data and suffer a personal data breach, the ICO will consider the extent to which you have put in place measures that PCI-DSS requires particularly if the breach related to a lack of a particular control or process mandated by the standard.

What do we do when a data processor is involved?

If one or more organisations process personal data on your behalf, then these are data processors under the GDPR. This can have the potential to cause security problems – as a data controller you are responsible for ensuring compliance with the GDPR and this includes what the processor does with the data. However, in addition to this, the GDPR's security requirements also apply to any processor you use.

This means that:

- you must choose a data processor that provides sufficient guarantees about its security measures;
- your written contract must stipulate that the processor takes all measures required under Article 32 – basically, the contract has to require the processor to undertake the same security measures that you would have to take if you were doing the processing yourself; and
- you should ensure that your contract includes a requirement that the processor makes available all information necessary to demonstrate compliance. This may include allowing for you to audit and inspect the processor, either yourself or an authorised third party.

At the same time, your processor can assist you in ensuring compliance with your security obligations. For example, if you lack the resource or technical expertise to implement certain measures, engaging a processor that has these resources can assist you in making sure personal data is processed securely, provided that your contractual arrangements are appropriate.

Further Reading

 [Relevant provisions in the GDPR - See Articles 28 and 32, and Recitals 81 and 83](#) 

External link

Should we use pseudonymisation and encryption?

Pseudonymisation and encryption are specified in the GDPR as two examples of measures that may be appropriate for you to implement. This does not mean that you are obliged to use these measures. It depends on the nature, scope, context and purposes of your processing, and the risks posed to individuals.

However, there are a wide range of solutions that allow you to implement both without great cost or difficulty. For example, for a number of years the ICO has considered encryption to be an appropriate technical measure given its widespread availability and relatively low cost of implementation. This position has not altered due to the GDPR – if you are storing personal data, or transmitting it over the internet, we recommend that you use encryption and have a suitable policy in place, taking account of

the residual risks involved.

When considering what to put in place, you should undertake a risk analysis and document your findings.

Further Reading

 [Relevant provisions in the GDPR - See Article 32\(1\)\(a\) and Recital 83](#) 

External link

In more detail – ICO guidance

We have published detailed [guidance on encryption](#) under the 1998 Act. Much of this guidance still applies, however we are also working to update it to reflect the GDPR.

What are ‘confidentiality, integrity, availability’ and ‘resilience’?

Collectively known as the ‘CIA triad’, confidentiality, integrity and availability are the three key elements of information security. If any of the three elements is compromised, then there can be serious consequences, both for you as a data controller, and for the individuals whose data you process.

The information security measures you implement should seek to guarantee all three both for the systems themselves and any data they process.

The CIA triad has existed for a number of years and its concepts are well-known to security professionals.

You are also required to have the ability to ensure the ‘resilience’ of your processing systems and services. Resilience refers to:

- whether your systems can continue operating under adverse conditions, such as those that may result from a physical or technical incident; and
- your ability to restore them to an effective state.

This refers to things like business continuity plans, disaster recovery, and cyber resilience. Again, there is a wide range of solutions available here, and what is appropriate for you depends on your circumstances.

Further Reading

 [Relevant provisions in the GDPR - See Article 32\(1\)\(b\) and Recital 83](#) 

External link

What are the requirements for restoring availability and access to personal data?

You must have the ability to restore the availability and access to personal data in the event of a physical or technical incident in a ‘timely manner’.

The GDPR does not define what a 'timely manner' should be. This therefore depends on:

- who you are;
- what systems you have; and
- the risk that may be posed to individuals if the personal data you process is unavailable for a period of time.

The key point is that you have taken this into account during your information risk assessment and selection of security measures. For example, by ensuring that you have an appropriate backup process in place you will have some level of assurance that if your systems do suffer a physical or technical incident you can restore them, and therefore the personal data they hold, as soon as reasonably possible.

Example

An organisation takes regular backups of its systems and the personal data held within them. It follows the well-known '3-2-1' backup strategy: three copies, with two stored on different devices and one stored off-site.

The organisation is targeted by a ransomware attack that results in the data being encrypted. This means that it is no longer able to access the personal data it holds.

Depending on the nature of the organisation and the data it processes, this lack of availability can have significant consequences on individuals – and would therefore be a personal data breach under the GDPR.

The ransomware has spread throughout the organisation's systems, meaning that two of the backups are also unavailable. However, the third backup, being stored off-site, allows the organisation to restore its systems in a timely manner. There may still be a loss of personal data depending on when the off-site backup was taken, but having the ability to restore the systems means that whilst there will be some disruption to the service, the organisation are nevertheless able to comply with this requirement of the GDPR.

Further Reading

 [Relevant provisions in the GDPR - See Article 32\(1\)\(c\) and Recital 83](#) 

External link

Are we required to ensure our security measures are effective?

Yes, the GDPR specifically requires you to have a process for regularly testing, assessing and evaluating the effectiveness of any measures you put in place. What these tests look like, and how regularly you do them, will depend on your own circumstances. However, it's important to note that the requirement in the GDPR concerns your measures in their entirety, therefore whatever 'scope' you choose for this testing should be appropriate to what you are doing, how you are doing it, and the data that you are processing.

Technically, you can undertake this through a number of techniques, such as vulnerability scanning and penetration testing. These are essentially 'stress tests' of your network and information systems, which are designed to reveal areas of potential risk and things that you can improve.

In some industries, you are required to undertake tests of security measures on a regular basis. The GDPR now makes this an obligation for all organisations. Importantly, it does not specify the type of testing, nor how regularly you should undertake it. It depends on your organisation and the personal data you are processing.

You can undertake testing internally or externally. In some cases it is recommended that both take place.

Whatever form of testing you undertake, you should document the results and make sure that you act upon any recommendations, or have a valid reason for not doing so, and implement appropriate safeguards. This is particularly important if your testing reveals potential critical flaws that could result in a personal data breach.

Further Reading

 [Relevant provisions in the GDPR - See Article 32\(1\)\(d\) and Recital 83](#) 

External link

What about codes of conduct and certification?

If your security measures include a product or service that adheres to a GDPR code of conduct (once any have been approved) or certification (once any have been issued), you may be able to use this as an element to demonstrate your compliance with the security principle. It is important that you check carefully that the code or certification is appropriately issued in accordance with the GDPR.

Further Reading

 [Relevant provisions in the GDPR - See Article 32\(3\) and Recital 83](#) 

External link

In more detail - Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The Article 29 Working Party will be producing specific guidance on certification in the coming months.

What about our staff?

The GDPR requires you to ensure that anyone acting under your authority with access to personal data does not process that data unless you have instructed them to do so. It is therefore vital that your staff understand the importance of protecting personal data, are familiar with your security policy and put its

procedures into practice.

You should provide appropriate initial and refresher training, including:

- your responsibilities as a data controller under the GDPR;
- staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority;
- the proper procedures to identify callers;
- the dangers of people trying to obtain personal data by deception (eg by pretending to be the individual whom the data concerns, or enabling staff to recognise 'phishing' attacks), or by persuading your staff to alter information when they should not do so; and
- any restrictions you place on the personal use of your systems by staff (eg to avoid virus infection or spam).

Your staff training will only be effective if the individuals delivering it are themselves reliable and knowledgeable.

Further Reading

 [Relevant provisions in the GDPR - See Article 32\(4\) and Recital 83](#) 

External link

Other resources

The NCSC has detailed [technical guidance](#)  in a number of areas that will be relevant to you whenever you process personal data. Some examples include:

- [10 Steps to Cyber Security](#)  – The 10 Steps define and communicate an Information Risk Management Regime which can provide protection against cyber-attacks.
- [The Cyber Essentials scheme](#)  – this provides a set of basic technical controls that you can implement to guard against common cyber threats.
- [Risk management collection](#)  – a collection of guidance on how to assess cyber risk.

The government has produced relevant guidance on cybersecurity:

- [CyberAware](#)  – a cross-government awareness campaign developed by the Home Office, the Department for Digital, Culture, Media and Sport ('DCMS') and the NCSC.
- ['Cybersecurity – what small businesses need to know'](#)  – produced by DCMS and the department for Business, Enterprise, Innovation and Skills ('BEIS').

Technical guidance produced by the European Union Agency for Network and Information Security (ENISA) may also assist you:

- [Data protection section](#)  at ENISA's website

In more detail – ICO guidance

The ICO and NCSC have jointly produced [guidance on security outcomes](#).

International transfers

At a glance

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

In brief

When can personal data be transferred outside the European Union?

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

What about transfers on the basis of a Commission decision?

Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

Further Reading

 [Relevant provisions in the GDPR - see Article 45 and Recitals 103-107 and 169](#) 

External link

What about transfers subject to appropriate safeguards?

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;

- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Further Reading

 [Relevant provisions in the GDPR - see Article 46 and Recitals 108-110 and 114](#) 

External link

Article 29 Working Party

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

According to its workplan, the Article 29 Working Party will publish guidelines on data transfers based on binding corporate rules and contractual clauses in 2017.

What about transfers based on an organisation's assessment of the adequacy of protection?

The GDPR limits your ability to transfer personal data outside the EU where this is based only on your own assessment of the adequacy of the protection afforded to the personal data.

Authorisations of transfers made by Member States or supervisory authorities and decisions of the Commission regarding adequate safeguards made under the Directive will remain valid/remain in force until amended, replaced or repealed.

Further Reading

 [Relevant provisions in the GDPR - see Articles 83 and 84 and Recitals 148-152](#) 

External link

Are there any derogations from the prohibition on transfers of personal data outside of the EU?

The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. A transfer, or set of transfers, may be made where the transfer is:

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;

- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

The first three derogations are not available for the activities of public authorities in the exercise of their public powers.

Further Reading

 [Relevant provisions in the GDPR - see Article 49 and Recitals 111 and 112](#) 

External link

What about one-off (or infrequent) transfers of personal data concerning only relatively few individuals?

Even where there is no Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that individual's rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU.

However, such transfers are permitted only where the transfer:

- is not being made by a public authority in the exercise of its public powers;
- is not repetitive (similar transfers are not made on a regular basis);
- involves data related to only a limited number of individuals;
- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

In these cases, organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals.

Further Reading

 [Relevant provisions in the GDPR - see Article 49 and Recital 113](#) 

External link

Further reading

 [Blog: Changes to Binding Corporate Rules applications to the ICO](#) 

External link

Personal data breaches

At a glance

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Checklists

Preparing for a personal data breach

- We know how to recognise a personal data breach.
- We understand that a personal data breach isn't only about loss or theft of personal data.
- We have prepared a response plan for addressing any personal data breaches that occur.
- We have allocated responsibility for managing breaches to a dedicated person or team.
- Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

- We have in place a process to assess the likely risk to individuals as a result of a breach.
- We know who is the relevant supervisory authority for our processing activities.
- We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
- We know what information we must give the ICO about a breach.
- We have a process to inform affected individuals about a breach when it is likely to result in a

high risk to their rights and freedoms.

- We know we must inform affected individuals without undue delay.
- We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.
- We document all breaches, even if they don't all need to be reported.

In brief

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify

the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:



"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Example

The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.

So, on becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

For more details about assessing risk, please see section IV of the Article 29 Working Party guidelines on personal data breach notification.

What role do processors have?

If your organisation uses a data processor, and this processor suffers a breach, then under Article 33(2) it must inform you without undue delay as soon as it becomes aware.

Example

Your organisation (the controller) contracts an IT services firm (the processor) to archive and store

customer records. The IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed. As this is a personal data breach, the IT firm promptly notifies you that the breach has taken place. You in turn notify the ICO.

This requirement allows you to take steps to address the breach and meet your breach-reporting obligations under the GDPR.

If you use a processor, the requirements on breach reporting should be detailed in the contract between you and your processor, as required under Article 28. For more details about contracts, please see our draft [GDPR guidance on contracts and liabilities between controllers and processors](#).

How much time do we have to report a breach?

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details of when a controller can be considered to have “become aware” of a breach.

What information must a breach notification to the supervisory authority contain?

When reporting a breach, the GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
 - the categories and approximate number of individuals concerned; and
 - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

What if we don't have all the required information available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

However, we expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify us of the breach when you become aware of it, and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to us and tell us when you expect to submit more information.

Example

You detect an intrusion into your network and become aware that files containing personal data have been accessed, but you don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system.

You notify the ICO within 72 hours of becoming aware of the breach, explaining that you don't yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the ICO more information about the breach without delay.

How do we notify a breach to the ICO?

To notify the ICO of a personal data breach, please see our [pages on reporting a breach](#).

Remember, in the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority. This means that as part of your breach response plan, you should establish which European data protection agency would be your lead supervisory authority for the processing activities that have been subject to the breach. For more guidance on determining who your lead authority is, please see the Article 29 Working Party [guidance on identifying your lead authority](#).

When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

Example

A hospital suffers a breach that results in an accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so they would need to be informed about the breach.

A university experiences a breach when a member of staff accidentally deletes a record of alumni contact details. The details are later re-created from a backup. This is unlikely to result in a high risk to the rights and freedoms of those individuals. They don't need to be informed about the breach.

If you decide not to notify individuals, you will still need to notify the ICO unless you can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. You should also remember that the

ICO has the power to compel you to inform affected individuals if we consider there is a high risk. In any event, you should document your decision-making process in line with the requirements of the accountability principle.

What information must we provide to individuals when telling them about a breach?

You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Does the GDPR require us to take any other steps in response to a breach?

You should ensure that you record all breaches, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires you to document the facts relating to the breach, its effects and the remedial action taken. This is part of your overall obligation to comply with the accountability principle, and allows us to verify your organisation's compliance with its notification duties under the GDPR.

As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

What else should we take into account?

The following aren't specific GDPR requirements, but you may need to take them into account when you've experienced a breach.

It is important to be aware that you may have additional notification obligations under other laws if you experience a personal data breach. For example:

- If you are a communications service provider, you must notify the ICO of any personal data breach within 24 hours under the Privacy and Electronic Communications Regulations (PECR). You should use our PECR breach notification form, rather than the GDPR process. Please see our [pages on PECR](#) for more details.
- If you are a UK trust service provider, you must notify the ICO of a security breach, which may include a personal data breach, within 24 hours under the Electronic Identification and Trust Services (eIDAS) Regulation. Where this includes a personal data breach you can use our [eIDAS breach notification form](#) or the GDPR breach-reporting process. However, if you report it to us under the GDPR, this still must be done within 24 hours. Please read our [Guide to eIDAS](#) for more information.
- If your organisation is an operator of essential services or a digital service provider, you will have incident-reporting obligations under the NIS Directive. These are separate from personal data breach notification under the GDPR. If you suffer an incident that's also a personal data breach, you will still need to report it to the ICO separately, and you should use the GDPR process for doing so.

You may also need to consider notifying third parties such as the police, insurers, professional bodies, or

bank or credit card companies who can help reduce the risk of financial loss to individuals.

The European Data Protection Board, which will replace the Article 29 Working Party, may issue guidelines, recommendations and best practice advice that may include further guidance on personal data breaches. You should look out for any such future guidance. Likewise, you should be aware of any recommendations issued under relevant codes of conduct or sector-specific requirements that your organisation may be subject to.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined with the ICO's other corrective powers under Article 58. So it's important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

Further Reading

 [Relevant provisions in the GDPR - See Articles 33, 34, 58, 83 and Recitals 75, 85-88](#) 
External link

In more detail - ICO guidance

See the following sections of the Guide to the GDPR:

- [Security](#)
- [Accountability and governance](#)

GDPR 'in more detail' guidance:

- [Draft GDPR guidance on contracts and liabilities between controllers and processors](#)

Existing DPA guidance:

- [Encryption](#)
- [A practical guide to IT security: ideal for the small business](#)

Other related guidance:

- [Guide to PECR](#)
- [Notification of PECR security breaches](#)
- [Guide to eIDAS](#)

In more detail - Article 29

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

Following the consultation period, the Article 29 Working Party has adopted final [guidelines on personal data breach notification](#).

The Article 29 Working Party has published [guidelines on lead supervisory authorities](#) and [lead supervisory authority FAQs](#).

Other resources

 [Report a security breach](#)
For organisations

Exemptions

What derogations does the GDPR permit?

Article 23 enables Member States to introduce derogations to the GDPR in certain situations.

Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.

What about other Member State derogations or exemptions?

Chapter IX provides that Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities. These include processing that relates to:

- freedom of expression and freedom of information;
- public access to official documents;
- national identification numbers;
- processing of employee data;
- processing for archiving purposes and for scientific or historical research and statistical purposes;
- secrecy obligations; and
- churches and religious associations.

Further Reading

 [Relevant provisions in the GDPR - see Articles 6\(2\), 6\(3\), 9\(a\)\(a\), 23 and 85-91 and Recitals 71, 50, 53 and 153-165](#) 

External link

Applications

To assist organisations in applying the requirements of the GDPR in different contexts, we are working to produce guidance in a number of areas. For example, children's data, CCTV, big data, etc.

This section will expand when our work on this guidance is complete.

Children

At a glance

- Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.
- If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.
- Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data.
- You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.
- If you are relying on consent as your lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent.(This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval).
- For children under this age you need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.
- Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.
- You should not usually make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them.
- You should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.
- Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

Checklists

General

- We comply with all the requirements of the GDPR, not just those specifically relating to children and included in this checklist.
- We design our processing with children in mind from the outset, and use a data protection by design and by default approach.
- We make sure that our processing is fair and complies with the data protection principles.
- As a matter of good practice, we use DPIAs to help us assess and mitigate the risks to

children.

- If our processing is likely to result in a high risk to the rights and freedom of children then we always do a DPIA.
- As a matter of good practice, we consult with children as appropriate when designing our processing.

Bases for processing a child's personal data

- When relying on consent, we make sure that the child understands what they are consenting to, and we do not exploit any imbalance in power in the relationship between us.
- When relying on 'necessary for the performance of a contract', we consider the child's competence to understand what they are agreeing to, and to enter into a contract.
- When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.

Offering an information Society Service (ISS) directly to a child, on the basis of consent

- If we decide not to offer our ISS (online service) directly to children, then we mitigate the risk of them gaining access, using measures that are proportionate to the risks inherent in the processing.
- When offering ISS to UK children on the basis of consent, we make reasonable efforts (taking into account the available technology and the risks inherent in the processing) to ensure that anyone who provides their own consent is at least 13 years old.
- When offering ISS to UK children on the basis of consent, we obtain parental consent to the processing for children who are under the age of 13, and make reasonable efforts (taking into account the available technology and risks inherent in the processing) to verify that the person providing consent holds parental responsibility for the child.
- When targeting wider European markets we comply with the age limits applicable in each Member state.
- We regularly review available age verification and parental responsibility verification mechanisms to ensure we are using appropriate current technology to reduce risk in the processing of children's personal data.
- We don't seek parental consent when offering online preventive or counselling services to a child.

Marketing

- When considering marketing children we take into account their reduced ability to recognise and critically assess the purposes behind the processing and the potential consequences of providing their personal data.
- We take into account sector specific guidance on marketing, such as that issued by the Advertising Standards Authority, to make sure that children's personal data is not used in a way that might lead to their exploitation.
- We stop processing a child's personal data for the purposes of direct marketing if they ask us to.
- We comply with the direct marketing requirements of the Privacy and Electronic Communications Regulations (PECR).

Solely automated decision making (including profiling)

- We don't usually use children's personal data to make solely automated decisions about them if these will have a legal, or similarly significant effect upon them.
- If we do use children's personal data to make such decisions then we make sure that one of the exceptions in Article 22(2) applies and that suitable, child appropriate, measures are in place to safeguard the child's rights, freedoms and legitimate interests.
- In the context of behavioural advertising, when deciding whether a solely automated decision has a similarly significant effect upon a child, we take into account: the choices and behaviours that we are seeking to influence; the way in which these might affect the child; and the child's increased vulnerability to this form of advertising; using wider evidence on these matters to support our assessment.
- We stop any profiling of a child that is related to direct marketing if they ask us to.

Privacy notices

- Our privacy notices are clear, and written in plain, age-appropriate language.
- We use child friendly ways of presenting privacy information, such as: diagrams, cartoons, graphics and videos, dashboards, layered and just-in-time notices, icons and symbols.
- We explain to children why we require the personal data we have asked for, and what we will do with it, in a way which they can understand.
- As a matter of good practice, we explain the risks inherent in the processing, and how we intend to safeguard against them, in a child friendly way, so that children (and their parents) understand the implications of sharing their personal data.
- We tell children what rights they have over their personal data in language they can understand.
- As a matter of good practice, if we are relying upon parental consent then we offer two different versions of our privacy notices; one aimed at the holder of parental responsibility and one aimed at the child.

The child's data protection rights

- We design the processes by which a child can exercise their data protection rights with the child in mind, and make them easy for children to access and understand.
- We allow competent children to exercise their own data protection rights.
- If our original processing was based on consent provided when the individual was a child, then we comply with requests for erasure whenever we can.
- We design our processes so that, as far as possible, it is as easy for a child to get their personal data erased as it was for them to provide it in the first place.

In brief

- [What's new?](#)
- [What should our general approach to processing children's personal data be?](#)
- [What do we need to think about when choosing a basis for processing children's personal data?](#)
- [What are the rules about an ISS and consent?](#)
- [What if we want to market to Children?](#)
- [What if we want to profile children or make automated decisions about them?](#)
- [How does the right to be informed apply to children?](#)
- [How does the right to erasure apply to children?](#)

What's new?

A child's personal data merits particular protection under the GDPR.

If you rely on consent as your lawful basis for processing personal data when offering an ISS directly to children, only children aged 13 or over are able provide their own consent. You may therefore need to verify that anyone giving their own consent in these circumstances is old enough to do so.

For children under this age you need to get consent from whoever holds parental responsibility for them - unless the ISS you offer is an online preventive or counselling service.

You must make reasonable efforts (using available technology) to verify that the person giving consent does, in fact, hold parental responsibility for the child.

Children merit specific protection when you are collecting their personal data and using it for marketing purposes or creating personality or user profiles.

You should not usually make decisions about children based solely on automated processing if this will have a legal or similarly significant effect on them. The circumstances in which the GDPR allows you to make such decisions are limited and only apply if you have suitable measures to protect the interests of the child in place.

You must write clear and age-appropriate privacy notices for children.

The right to have personal data erased is particularly relevant when the individual gave their consent to processing when they were a child.

What should our general approach to processing children's personal data be?

Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.

If you process children's personal data, or think that you might, then you should consider the need to protect them from the outset, and design your systems and processes with this in mind.

Fairness, and compliance with the data protection principles, should be central to all your processing of children's personal data.

It is good practice to consult with children when designing your processing.

What do we need to think about when choosing a basis for processing children's personal data?

As with adults, you need to have a lawful basis for processing a child's personal data and you need to decide what that basis is before you start processing.

You can use any of the lawful bases for processing set out in the GDPR when processing children's personal data. But for some bases there are additional things you need to think about when your data subject is a child.

If you wish to rely upon consent as your lawful basis for processing, then you need to ensure that the child can understand what they are consenting to, otherwise the consent is not 'informed' and therefore invalid. There are also some additional rules for online consent.

If you wish to rely upon 'performance of a contract' as your lawful basis for processing, then you must consider the child's competence to agree to the contract and to understand the implications of this processing.

If you wish to rely upon legitimate interests as your lawful basis for processing you must balance your own (or a third party's) legitimate interests in processing the personal data against the interests and fundamental rights and freedoms of the child. This involves a judgement as to the nature and purpose of the processing and the potential risks it poses to children. It also requires you to take appropriate measures to safeguard against those risks.

What are the rules about an ISS and consent?

Consent is not the only basis for processing children's personal data in the context of an ISS.

However, if you do rely upon consent as your lawful basis for processing personal data when offering an ISS directly to children, in the UK only children aged 13 or over can consent for themselves. (This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval). You therefore need to make reasonable efforts to verify that anyone giving their own consent in this context is old enough to do so.

For children under this age you need to get consent from whoever holds parental responsibility for them - unless the ISS you offer is an online preventive or counselling service.

You must make reasonable efforts (using available technology) to verify that the person giving consent does, in fact, hold parental responsibility for the child.

You should regularly review the steps you are taking to protect children's personal data and consider whether you are able to implement more effective verification mechanisms when obtaining consent for processing.

What if we want to market to children?

Children merit specific protection when you are using their personal data for marketing purposes. You should not exploit any lack of understanding or vulnerability.

They have the same right as adults to object to you processing their personal data for direct marketing. So you must stop doing this if a child (or someone acting on their behalf) asks you to do so.

If you wish to send electronic marketing messages to children then you also need to comply with the Privacy and Electronic Communications Regulations 2003.

What if we want to profile children or make automated decisions about them?

In most circumstances you should not make decisions about children that are based solely on automated processing, (including profiling) if these have a legal effect on the child, or similarly significantly affect them.

The GDPR gives children the right not to be subject to this type of decision. Although there are exceptions to this right, they only apply if suitable measures are in place to protect the rights, freedoms and legitimate interests of the child.

If you profile children then you must provide them with clear information about what you are doing with their personal data. You should not exploit any lack of understanding or vulnerability.

You should generally avoid profiling children for marketing purposes. You must respect a child's absolute right to object to profiling that is related to direct marketing, and stop doing this if they ask you to.

It is possible for behavioural advertising to 'similarly significantly affect' a child. It depends on the nature of the choices and behaviour it seeks to influence.

How does the right to be informed apply to children?

You must provide children with the same information about what you do with their personal data as you give adults. It is good practice to also explain the risks inherent in the processing and the safeguards you have put in place.

You should write in a concise, clear and plain style for any information you are directing to children. It should be age-appropriate and presented in a way that appeals to a young audience.

If you are relying upon parental consent as your lawful basis for processing it is good practice to provide

separate privacy notices aimed at both the child and the responsible adult.

If you provide an ISS and children younger than your target age range are likely to try and access it then it is good practice to explain any age limit to them in language they can understand.

Children have the same rights as adults over their personal data and can exercise their own rights as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may exercise the child's data protection rights on their behalf.

How does the right to erasure apply to children?

Children have the same right to have their personal data erased as adults.

This right is particularly relevant when an individual originally gave their consent to processing when they were a child, without being fully aware of the risks.

One of the specified circumstances in which the right to erasure applies is when you collected the personal data of a child under the lawful basis of consent, when offering an ISS directly to a child.

It should generally be as easy for a child to exercise their right to erasure as it was for them to provide their personal data in the first place.

Further Reading

 [Relevant provisions in the GDPR - See Articles 8, 12\(1\) and 17\(1\)\(f\) and Recitals 38, 58, 65, and 71](#) 
External link

In more detail - ICO guidance

We have published [detailed guidance on Children and the GDPR](#) for public consultation. The consultation closes on 28 February 2018.

Safeguarding children and protecting professionals in early years settings: online safety considerations

Published 4 February 2019

Contents

1. Policies and Procedures
2. Infrastructure and Technology
3. Education and Training
4. Standards and Monitoring
5. Additional Information and Support

This document is to help managers of early years settings (including wrap around care for the early years age group) ensure their online safeguarding practice is in line with statutory requirements and best practice. It may be helpful for managers to access and share with staff the [‘Online Safety Guidance for Practitioners’](#) guidance.

- All early years providers in England must follow the [Early Years Foundation Stage \(EYFS\)](#); there are different early years standards in [Scotland](#) and Wales.
- Providers must have regard to the government’s statutory guidance [‘Working Together to Safeguard Children’ 2018](#) and to the [‘Prevent duty guidance for England and Wales’ 2015](#).
- Maintained nursery schools must have regards to [‘Keeping Children Safe in Education’ \(KCSIE\) 2018 statutory guidance](#); other childcare providers may also find it helpful to refer to this guidance.

1. Policies and Procedures

1.1 Why do early years settings need to consider this?

EYFS 2017

- If providers have concerns about children’s safety or welfare, they must notify agencies with statutory responsibilities without delay
- The setting’s safeguarding policy and procedures must cover the use of mobile phones and cameras in the setting.
- There is an expectation that children can access technology and use it safely.

Ofsted ‘Inspecting Safeguarding’ 2018

- Leaders oversee the safe use of technology when children and learners are in their care and take action immediately if they are concerned about bullying or children's well-being.
- Leaders of early years settings implement the required policies with regard to the safe use of mobile phones and cameras in settings.

1.2 Managers should evidence that:

- Online safety is recognised as part of the setting's safeguarding responsibilities - the Designated Safeguarding Lead (DSL) should take lead responsibility for online safety concerns.
- Online safety concerns are reported to the DSL, recorded and actioned.
- Children are enabled (at a level appropriate to their age and ability) to share online concerns
- The child protection policy includes procedures to follow regarding online safety concerns
- Their settings policies cover: Safe and appropriate use of personal devices, wearable technology, mobile phones and cameras;
Acceptable and appropriate use of technology within the setting;
Expectations regarding professional boundaries/behaviour of staff, including communication via social media
- Policies and procedures are easily accessible to staff and parents/carers, for example, published on the setting's website.
- Staff and parents/carers are consulted and actively involved, as far as possible in the development of policies
- Policies have been reviewed and approved by the management team/committee or equivalent

1.3 Managers should ensure that all staff:

- Understand their safeguarding responsibility and are clear about how it fits into their role on a day to day basis
- Have read and understood the setting's policies relevant to online safety - this should include an Acceptable Use Policy (AUP) as part of the settings code of conduct.

- Are familiar with the setting's policies and procedures regarding safe technology use with children.
- Are aware of the policy regarding staff contact outside of work;
- Communication with learners, parents/carers and colleagues should be professional and take place via official setting communication channels e.g. work provided emails/numbers to protect both staff and learners
- Communication should be transparent and open to scrutiny - settings may find it helpful to access ['Guidance for safer working practice for those working with children and young people in education settings'](#)
- Understand that it is recommended that staff do not accept friend requests or communications from learners or their family members (past or present). If there is a pre-existing relationship, this should be discussed with the DSL and/or the manager, who will need to consider how this is managed, provide staff with clear guidance and boundaries and record action taken.
- Understand and follow the procedures for reporting and recording online safety concerns, in line with the child protection policy.
- Make use of home visits to inform their understanding of a child's context with regards to technology within the home. (e.g. how much and in what ways is tech used within the child's family life?)
- Are aware that if they or another member of staff are targeted online, for example online bullying or harassment they should inform their line manager. Managers may find it helpful to access the DfE ['Cyberbullying: Advice for headteachers and school staff'](#) guidance.
- Are clear on the internal and external reporting mechanism regarding online safety concerns. Staff should always involve the DSL who will be able to make decisions about how and when to escalate a concern.
- Know how to access the settings whistleblowing policy and the [NSPCC whistleblowing helpline](#)

DSLs and staff should know how to contact:

- your local Multi-Agency Safeguarding Hub if they have a safeguarding concern about a child;
- the [Internet Watch Foundation](#) (IWF) if settings need to report illegal images (child sexual abuse material);

- the [Child Exploitation and Online Protection centre \(CEOP\)](#) if they are worried about online abuse or the way that someone has been communicating online;
- the [UK Safer Internet Centre Helpline for Professionals](#) or the [NSPCC](#) for further information.

2. Infrastructure and Technology

2.1 Why do early years settings need to consider this?

Prevent Duty (2015)

- Schools (and registered childcare providers) in England and Wales are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering”.
- Ofsted ‘Inspecting Safeguarding’ 2018: Appropriate filters and monitoring systems are in place to protect learners from potentially harmful online material

2.2 Managers should evidence that:

- They are aware of how and why technology is used within the setting by staff and children. This should include types and number of devices, if they are connected to the internet and if so, how (e.g. Wi-Fi)
- Access to the setting’s network and IT infrastructure is secure, such as use of passwords, screen locks, protected devices if removed from site
- Appropriate filtering and monitoring are in place and the setting has documented how decisions have been made; advice regarding appropriate filtering and monitoring is available from the [UK Safer Internet Centre](#)
- Access to setting’s devices is managed and monitored

- Setting's devices are kept securely and in line with data protection requirements.
- Physical safety of users has been considered e.g. posture of children/staff when using devices.
- Personal data is managed securely online, in accordance with the statutory requirements of the General Data Protection Regulations (GDPR) and Data Protection legislation.
- This should include considerations given to the use of online learning journals or apps if used.

-

2.3 Managers should ensure that all staff:

- Appropriately supervise children whenever they are using devices
- Check apps, websites and tools prior to using them with children, this should include checking the results of searches
- Use age appropriate apps, websites and online tools with children - there are details of useful websites that will provide links to appropriate content at the end of the document
- Model safe practice when using technology with children
- Ensure data is shared online in accordance with the settings data protection responsibilities

3. Education and Training

3.1 Why do early years settings need to consider this?

EYFS 2017

- Providers must train all staff to understand their safeguarding policy and procedures and ensure that all staff have up to date knowledge of safeguarding issues.

Ofsted 'Inspecting Safeguarding' 2018

- Staff, leaders and managers oversee the safe use of electronic and social media by staff and learners and take action immediately if they are concerned about bullying or risky behaviour.

-

3.2 Managers should evidence that:

- The DSL has accessed training/information to ensure they understand the unique risks associated with online safety for early years children and have the relevant knowledge and up to date capability required to keep children safe online Managers should ensure that all staff:
 - Are provided with quality and up-to-date online safety training on a regular (at least annual) basis, including at induction.
 - Are aware of the UKCIS framework (Education for a Connected World) which provides information about the skills and competences that children and young people need to have with regards to online safety from the age of 4 upwards.
 - Know how to report a problem and when to escalate a concern.
 - Are aware that civil, legal or disciplinary action can be taken against staff if they are found to have brought the profession or institution into disrepute.
 - Are aware that under no circumstances should any member of staff, either at work or in any other place, make, deliberately download, possess, or distribute material they know to be illegal, for example child sexual abuse material.
 - Are aware of the need to manage their digital reputation, including the appropriateness of information and content that they post online, both professionally and personally.
 - Discuss online expectations and behaviour with their friends and colleagues - for example, have they discussed what photos of them can and cannot be shared by their friends on social media.
 - Are aware that no matter what privacy settings are used, anything posted online can become public and permanent and could be misinterpreted and/or used without their knowledge or consent. Managers should ensure that all children:
 - Receive age appropriate, progressive and embedded online safety education throughout the curriculum.
 - Use age appropriate tools and resources.

3.3 Managers should ensure that parents:

- Are given opportunities to develop their knowledge of online safety issues for early years children.
- Are offered support to help them talk about online safety with their children in an age appropriate way.
- Are signposted to appropriate sources of support regarding online safety at home.
- Are supported by the setting if they experience an online safety concern.

4. Standards and Monitoring

4.1 Why do early years settings need to consider this?

Ofsted 'Inspecting Safeguarding' 2018

- Leaders oversee the safe use of technology when children and learners are in their care and take action immediately if they are concerned about bullying or children's well-being.
-

4.2 Managers should evidence that:

- Policies are updated at least annually, and following any local/national changes
- The setting regularly monitors and evaluates online safety approaches e.g. reflecting on concerns and updating practice
- Staff are trained and provided with regular (at least annual) updates on online safety issues

5. Additional Information and Support

Many local authorities and grids provide in depth guidance and template policies to support managers and designated safeguarding leads within early years settings; check to see what support and training is available locally to you.

The following national organisations provide information:

- Childnet: For a range of educational materials and resources for use with children, parents and teachers, including [‘Social networking: a guide for teachers and professionals’](#) and [‘Keeping young children safe online’](#)
- [DfE Data Protection Toolkit for Schools](#): For information on what schools need to do in order to comply with data protection regulations
- [Information Commissioners Office](#) (ICO): For information around data protection and GDPR
- Internet Matters: For a range of materials for parents and teachers, including for [pre-school](#) and [0-5](#)
- NCA-CEOP: Education resources for use with children, parents and professionals and advice on safeguarding children from sexual abuse, including www.thinkuknow.co.uk and the [CEOP Safety Centre](#)
- [NSPCC online safety](#)
- [Parent Zone](#): For a range of education materials and resources for use with children, parents and teachers
- [Parent Info](#)
- [UK Safer Internet Centre](#): For a range of education materials and resources for use with children, parents and [teachers](#), UK SIC helpline for professionals who are working with children and young people

Acceptable Use and Policy templates:

- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety
- <https://swgfl.org.uk/products-services/online-safety/resources/online-safety-policy-templates/>
- safepolicies.lgfl.net

This document has been bought to you by the UKCIS Education Working Group.

Personal data an employer can keep about an employee.

Employers must keep their employees' personal data safe, secure, and up to date.

Employers can keep the following data about their employees without their permission:

- name
- address
- date of birth
- sex
- education and qualifications
- work experience
- National Insurance number
- tax code
- emergency contact details
- employment history with the organisation
- employment terms and conditions (e.g., pay, hours of work, holidays, benefits, absence)
- any accidents connected with work.
- any training taken.
- any disciplinary action

Employers need their employees' permission to keep certain types of 'sensitive' data, including:

- race and ethnicity
- religion
- political membership or opinions
- trade union membership
- genetics

- biometrics, for example if your fingerprints are used for identification.
- health and medical conditions
- sexual history or orientation

Employers must keep sensitive data more securely than other types of data.

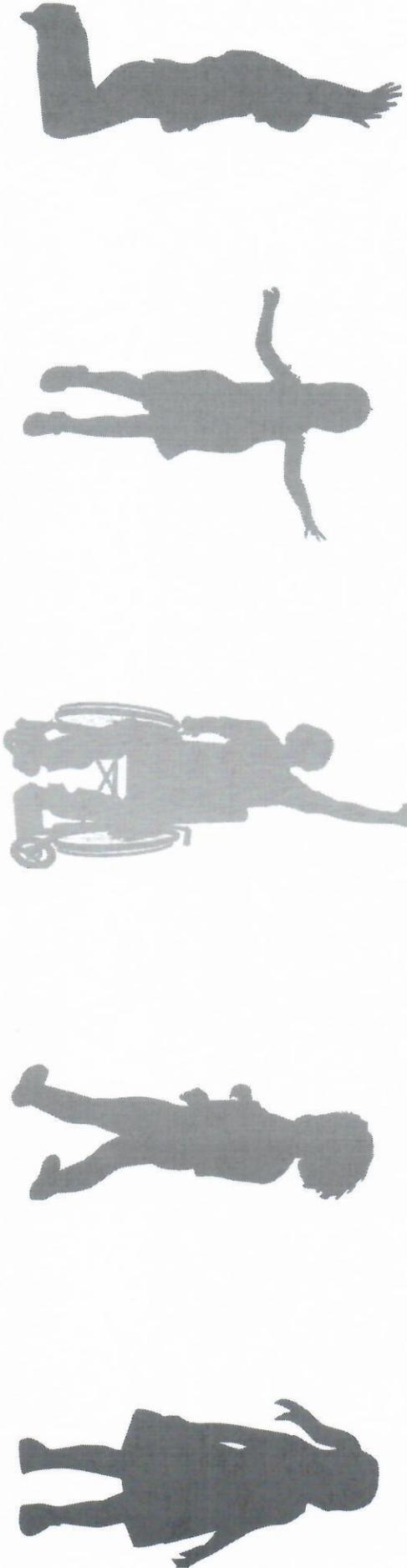
What an employer should tell an employee

An employee has a right to be told:

- what records are kept and how they are used?
- the confidentiality of the records
- how these records can help with their training and development at work

If an employee asks to find out what data is kept on them, the employer will have 30 days to provide a copy of the information.

An employer should not keep data any longer than is necessary and they must follow the [rules on data protection](#).



Liverpool Safeguarding Children Board

Working together to promote children's welfare and provide early help

Responding to Need Guidance and Levels of Need Framework

Need Description 1.1.2016



Index

Introduction.....	2
What is Early Help?.....	3
How to use the Levels of Need Framework.....	4
Promoting Children's Wellbeing through early help in Liverpool (windscreen model).....	6
Understanding Levels of Need.....	7
Determinants of Need	8
Development of baby (inc.unborn), child or young person.....	8
Parents and Carers	10
Family and Environment	11
Liverpool's Route to support.....	12
Good Practise Prompts	15
Useful Links.....	16

Introduction

Liverpool Safeguarding Children Board's (LSCB) 'Responding to Need Guidance' has been designed with partners from across the Children's Trust and the LSCB to ensure that children's needs are responded to at an appropriate level and in a timely way. This guidance should be seen as overarching guidance for the whole of the children and young people's workforce within Liverpool. It is a guide for all agencies, professionals and volunteers, to consider how best to meet the needs of individual children. Individual agency response to levels of needs will vary depending on the individual agency but their responses should all support this framework, and deliver appropriate interventions for children and families.

PARTNERSHIPS AND JOINT WORKING ARE KEY TO ENSURING POSITIVE OUTCOMES FOR CHILDREN, AND TO REDUCE THE NEED FOR MORE INTENSE INTERVENTIONS AT A LATER STAGE.

This document replaces the previous version of this document published July 2014. The name of the guidance has been changed to place greater emphasis on responding to 'levels of need' and specifically focus on improving outcomes for children at the earliest opportunity, through effective partnership working with families and partner agencies. The Early Help Assessment is the agreed framework that supports partnerships/joint working and multi-agency interventions which are recorded on the Early Help Assessment Tool documentation (EHAT).

liverpool.gov/EHAT

This framework follows the 'windscreen model' which illustrates when services begin from early help to statutory intervention.

The aim is that as far as possible, children's needs should be met within universal provision, but where additional needs are identified, flexible support should be introduced at the earliest opportunity, with parental [and/or child where age appropriate] consent, thus alleviating problems that have started to emerge, prevent problems from escalating and help to improve outcomes.

This guidance will assist all agencies and professionals effectively and accurately assess levels of need and/or risk of children and families in Liverpool so that a timely response is provided by services to meet the level of assessed need.

Working Together to Safeguard Children (2015) gives responsibility to Safeguarding Children Boards to assess the effectiveness of early help offered to families and whether agencies are fulfilling their statutory obligation to work together to provide the early help assessment. LSCBs are also required to publish local protocols for assessment of need, including how the need is identified and met through an agreed shared process. In Liverpool, this is now referred to as the Early Help Assessment Tool (EHAT), and Single Assessment as the statutory assessment of the Local Authority.

In some circumstances, a child's and family's needs and levels of concern may not be met through coordinated early help, and consequently there may be need to provide more intensive or specialist support lead by social care. The term 'step up' is often used to describe this process.

Equally, the term 'step down' is used to describe children and families moving from a high level of intervention, including statutory intervention, to a lower level of coordinated support. This is important in ensuring that issues do not re-escalate.

What Is Early Help?

Early Help refers both to help in the critical early years of a child's life, when the fundamental building blocks of future development are laid, and also help throughout a child, young person and family's life too. This should happen as soon as possible when difficulties emerge in order to prevent problems from becoming entrenched or escalating. Early help is underpinned with Universal Services to identify the need for support at an early stage for those families who may need it.

Effective early help may occur at any point in a family's life, from prebirth to teenage years. The development of an effective early help offer is the responsibility of all strategic partners, and is a responsibility shared with families and their communities.

Our ambition is that families, particularly those with multiple and complex needs, will have access to co-ordinated early help in accordance with need as soon as difficulties are identified. This support should be personalised, multi-agency, evidence based and embedded within a whole family approach. Children and young people in those families will be supported to live safe, healthy and fulfilling lives, and to develop into responsible adult citizens. Early help can break the intergenerational cycle of risk and vulnerability. Families will become more resilient and develop capabilities to prevent and resolve problems themselves.

Early help can reduce demand for higher cost specialist services and achieve greater use of community based universal preventative services. Families and local communities will become resilient through early help.

There are occasions when professionals have concerns relating to extremism/and or harmful practices. In most cases, these can be supported with early help interventions, through partnership working across agencies.

However, there is a statutory need to inform social care services when these concerns arise, and the practitioner identifying those concerns may want to seek specialist advice on how to manage further support. In those cases, Careline can be contacted to report a concern relating to extremism or harmful practices, and those concerns will be recorded and relevant advice given in order to maintain the appropriate level of support for the family.

For further information, see Liverpool's Integrated Early Help Strategy <http://liverpool.gov.uk/council/strategies-plans-and-policies/children-and-families/early-help-strategy/>

How to use the Levels of Need Framework

This is a guide for practitioners and managers in every agency that works with, or is involved with children, young people and their families. The framework follows the 'windscreen model' illustrated within this document. Its' aim is to assist practitioners and managers in assessing and identifying a child's level of need; what type of service/ resources may meet those needs, and the process to follow in moving from an identification of need to provision of services. It is important that all agencies understand the needs of each individual child within their own context and realise that each child's situation is unique and specific to them. What follows is therefore a guide for clarification to assist professional judgements in determining the next actions in meeting those needs.

It is crucial to ensure a range of service provision is available to meet the needs of children in the community and to ensure that the appropriate services are accessed to meet those needs in a strong integrated manner.

The framework and approach adopted is underpinned by the following principles:

- Children in levels 2-4 also need and use universal services
- Children's needs can move from one level to another, and it should not be necessary for those needs to be captured more than once.
- Children should be enabled to move quickly and effortlessly to the required service response without necessarily going through each level.

- Where needs appear to have been met, families should be able to choose to keep an open (suspended) Early Help Assessment Tool, (formerly known as CAF) so they can share with services should needs re-emerge at a later stage.

- Children and young people have a right to have their voice heard

– and this should have a strong influence on what happens next

There will be times when there are differences of views/perceptions how best to support a child and family and the levels of intervention required by different agencies. In the first instance, this should be resolved with the multi-agency group, and if agreement is not reached and cases become 'stuck' then the practitioner who disagreed with the outcome should notify their manager, who in turn should consult and use the escalation process.

This process is based on agencies assessing and describing the needs of the child by using the Early Help Assessment Tool or by contacting Careline and providing information to request statutory service support using the multi-agency form. Reference should always be made to this Responding to Need Guidance and Levels of Need Framework.

This framework is designed to help everyone to:

- think clearly and achieve a holistic approach
- understand the child in the context of their family and wider community
- develop ideas and solutions with children and their families, so that timely support is provided at the right level.

The framework describes how the Early Help Assessment Tool (EHAT) can be used by all services to provide the holistic overview of needs, and if necessary, to inform statutory assessments where needs require acute or specialist support.

- At levels 2 & 3, the framework describes the Team Around the Child/ Family approach, which is facilitated by a Lead Professional.
- Level 4 describes children with acute specialist needs where statutory assessments are required

In these cases the Local Authority Children's Social Care Services leads and assesses the needs of the child alongside other professionals using a Single Assessment.

Agencies working with children and their families should always aim to support identified needs within their own agency or in partnership with other agencies or services.

Where acute/specialist service needs have been identified, a social care single assessment is required. An Early Help Assessment Tool will inform the Single Assessment.

If needs escalate beyond early help and require statutory intervention, Careline should be contacted to discuss the best way to meet those needs.

The term 'step up' and 'step down' is commonly used to describe children moving between levels of need and is used within the framework to describe the process by which children's needs can change. This requires all professionals working with children and their families to be familiar with the approach so that if and when a service is terminated, due to a change in need, there is a clear and agreed response for service support.

It is recognised that the service and agency arrangements will continue to change as organisations respond to local and national priorities. However, the principles of partnership working and holistic support for families remains constant.

Many agencies are constantly reviewing how their services can be adapted to deliver a more localised support and provide a neighbourhood model of delivery that supports families in their communities.

It is vital that every professional sees how their role can often be a 'contribution' to the support of a child in the family, and that the broader support from partners is what is key to making the difference for families, and preventing concerns escalating and requiring statutory social care interventions.

Although consent is required for completion of an EHAT, where this is stated throughout this document, you are reminded that consent is not needed where there are safeguarding concerns or there may be legal powers permitting the sharing of information. Practitioners working with families undertaking an Early Help Assessment should always explain clearly what the consent statement means for the avoidance of any misunderstandings.

Promoting Children's Wellbeing in Liverpool - Levels of Need as a Continuum



Effective Information Sharing

Contact Careline immediately for concerns that a child has suffered or is likely to suffer significant harm. (Level 4) or where you are not certain.

The windscreen model is used for illustration only and does not necessarily reflect the proportions of families within Liverpool that under the level of needs described. Consent is always the needed when offering single or multi-agency support to families and parental engagement is fundamental. This enables effective sharing of information and appropriate support being put in place regardless of the level of need. However, consent is not needed when there are significant welfare concerns or likely risk/harm for a child

Understanding Levels of Need

Consent: Gaining consent from parent(s) to participate in decisions about supporting identified needs and the sharing information is good practice. This enables a swift and most supportive response in the timely engagement of relevant services/agencies. Gaining consent is best practice at all levels of need. However, where consent is not obtained, a professional judgement is needed in relation to assessed risk and significant harm, which will inform a decision to make contact with Careline to discuss a referral. Where concerns relate to potential significant harm or risk to a child's welfare, gaining consent should not be a barrier to discussing those concerns with practitioner's line management and respective agency safeguarding procedures.

Level 1: Universal services

Children and young people make good overall progress in all areas of development. These children receive appropriate universal services, such as health, care and education. They may also use leisure and play facilities, housing or voluntary sector services. These children may have a single identified need that can be adequately met by a universal service. However, if further additional needs are identified, an Early Help Assessment (formerly known as a CAF) will be required to step up to Level 2 or 3.

Level 2: Early Help Multi-Agency Support (More than a single service)/Children and young people who require some extra support/intervention. This may be short term, but requires a co-ordinated response from services. Children and young people will benefit from an Early Help Assessment/Team Around the Child (or Family) arrangement to ensure needs are met and escalation of need is minimised. An Early Help Assessment will also ensure that information is held centrally and visible (with consent) to other professionals who may also have concerns.

Level 3: Complex Needs, Targeted Support Children and young people with un-met needs that are more significant or complex. Early Help and a co-ordinated multi-agency response to needs can prevent concerns escalating to a level that may require statutory interventions. The Early Help Assessment and subsequent Team Around the Child (TAC) or Family (TAF) identifies a lead professional, and ensures support is appropriate and timely and impact is measured. Where concerns escalate beyond early help, and significant harm is likely or a child's level of development/welfare is compromised, the concern can be 'stepped up' for social care interventions where appropriate. Similarly, where there has been social care interventions, and needs have been addressed, it can be 'stepped down' to ensure continuation of support that is appropriately provided through multi-agency arrangements, which should prevent re-escalation at a later stage.

Level 4: Acute and Specialist Needs: Safeguarding/Statutory Social Care Services (Careline referral accepted) Children and young people who are 'in need' and require a statutory service to promote their welfare (section 17), and children and young people whose needs demonstrate significant harm or risk of significant harm (section 47). Needs at Level 4 are complex and cross many domains/determinants. These are cases of a Childprotection nature where there is 'reasonable cause' to suspect suffering or likely suffering of significant harm. This includes concerns where a child may be exposed to harmful practices or extremism. These are cases of a Child Protection nature where there is 'reasonable cause' to suspect suffering or likely suffering of significant harm, (as defined by Children Act). They will be co-ordinated and led by a Social Worker. The Early Help/Team around the Child (or Family) process will be used to 'step down' to a lower level when the level of risk and/or need reduces.

Determinants of Need (an indication of factors affecting needs)

Determinant

Level 1

Level 2

Level 3

Level 4

Universal

Additional Needs Multi Agency
Early Help Assessment

Complex Targeted
Early Help Assessment

Acute / Specialist
Careline

Health

- Physically well
- Adequate diet/hygiene/clothing
- Developmental checks/immunisations up to date
- Regular dental/optical care
- Health appointments kept
- Speech and language development met

- Defaulting on immunisation checks
- Susceptible to minor health problems
- Slow in reaching developmental milestones
- Minor concerns re: diet/hygiene/lack of sleep
- Smokes/ alcohol concerns
- Starting to default on health appointments
- Presenting with inappropriate sexualised behaviour
- Teenage pregnancy (consider age and social circumstances)

- Concerns re: diet, hygiene, clothing
- Some chronic health problems
- Missing routine and non-routine health appointments
- Substance misuse
- Developmental milestones are unlikely to be met
- Concerns around mental health
- Teenage pregnancy (multi-agency response) (consider age and social circumstances)
- Significant change in mood
- Recurring health problems
- Promiscuity

- Severe/chronic health problems
- Persistent substance misuse
- Developmental milestones are unlikely to
- Teenage pregnancy (acute level of need)
- Serious mental health issues
- No engagement with Health professionals

Education and Learning

- Skills interest
- Success/achievement
- Cognitive development
- Access to books and toys, play
- Choices and encouragement

- Some identified learning or physical disability needs, requiring support
- Poor punctuality
- Pattern of school absences
- Not always engaged in learning – poor concentration/low motivation/interest
- Not reaching educational potential
- Limited access to books/toys
- High levels of school mobility

- Significant learning needs and may have Statement or Educational needs (or Education Health Care Plan)
- Poor school attendance and punctuality
- Some fixed term exclusions
- Not engaged in education or reaching educational potential
- Fear of holidays, leaving school
- Pre-occupied with ideology

- Out of School
- Permanently excluded from school or at risk of permanent exclusion
- No access to leisure activities

Emotional and Behavioural Development

- Feelings/actions demonstrate appropriate responses
- Good quality early attachments
- Able to adapt to change
- Able to demonstrate empathy

- Some difficulties with peer group relationships and adults
- Concern of self-harm (including substance misuse)
- Some evidence of inappropriate responses and actions
- Can find managing change difficult
- Starting to show difficulties expressing empathy
- Low self-esteem/self confidence
- Feelings: Grievance/ Injustice/oppression

- Finds it difficult to cope with anger, frustration and upset
- Disruptive/challenging behaviour at school or in neighbourhood
- Cannot manage change
- Unable to demonstrate empathy
- Repeated episodes of self-harm and/or substance misuse

- Regularly involved in anti-social/criminal activities
- Puts self or others in danger e.g. missing from home or in care
- Suffers from periods of depression
- Suicide attempts
- Children at risk of sexual exploitation
- Harmful Objectives
- Manipulation and coercion into negative religious activities

Determinant

Level 1

Level 2

Level 3

Level 4

Universal

Additional Needs Multi Agency Early Help Assessment

Complex Targeted Early Help Assessment

Acute / Specialist Careline

Identity

- Positive sense of self and abilities
- Demonstrates feelings of belonging and acceptance
- Sense of self
- Ability to express needs

- Some insecurities around identity expressed (confusion linked to culture, isolation, threatened), low self-esteem for learning
- May experience bullying around "differences"
- Unsure or unable to disclose sexual orientation
- May be affected by peer/gang pressure
- Strong negative gender identification and roles

- Is subject to discrimination e.g. racial, sexual orientation or disabilities
- Demonstrates significantly low self-esteem in a range of situations
- Is subject to peer/gang pressure
- Serious negative belief systems about gender.
- Marginalised/over identification with group or ideology.
- Us and them mindset
- Religion, culture

- Experiences persistent
- Discrimination e.g. racial, sexual orientation disability
- Involved with organised gangs or criminal activity
- Discriminating on grounds of gender, cultural religious identity

Family and Social Relationships

- Stable, affectionate with care givers
- Good relationships with siblings
- Positive relationships with peers

- Some support from family and friends
- Some difficulties sustaining relationships
- Gang associations through relatives, peers or relationship
- Signs of being bullied
- Age inappropriate relationships
- Self isolation from family
- Family attitude justify offending

- Has lack of positive role models
- Misses school or leisure activities
- Peers also involved in challenging behaviour
- Involved in conflict with peers/siblings
- Regularly needed to care for another family member
- Manipulation and coercion to comply with negative gender, religion, cultural behaviours
- Known gang involvement
- Little social relationships outside the home
- Family/Friends involved in extremism
- Access to extremist networks

- Periods of being accommodated by the LA Authority
- Family breakdown related in some way to behavioural difficulties
- Subject to physical, emotional or sexual abuse or neglect
- Main carer for family member
- Unaccompanied asylum seeker
- Where parents have made private fostering arrangements
- Involved in manipulation and coercion of care
- Known involvement with extremist group

Social Presentation

- Appropriate dress for different circumstances
- Good level of personal hygiene
- Can choose own clothing

- Can be over-friendly or withdrawn with strangers
- Can be provocative in appearance and behaviour
- Personal hygiene starting to be a problem
- Unexplained change in peer group – can be dominated

- Is provocative in behaviour/appearance
- Clothing is regularly unwashed
- Hygiene problems
- Sudden display of unexplained gifts / clothing
- Attitudes justify offending
- Intolerant of other's views – resulting in de-humanising of perceived enemies

- Poor and inappropriate self-presentation

Self-care Skills

- Growing level of competencies in practical and emotional skills such as feeding, dressing and independent living skills

- Not always adequate self-care e.g. poor hygiene, self neglect
- Slow to develop age-appropriate self-care skills

- Poor self-care for age, including hygiene
- Inappropriately able to care for self
- Pre-occupation with the internet

- Neglects to use self-care skills due to alternative priorities e.g. substance misuse

B. Parents and Carers

Level 1

Universal

Basic Care

- Provides for child's physical needs e.g. food, drink, appropriate clothing, medical and dental care

Level 2

Additional Needs Multi Agency Early Help Assessment

- Engagement with services is poor
- Requires advice on parenting issues
- Professionals are beginning to have some concerns around child's physical needs being met
- Parental decisions affecting child safety

Level 3

Complex Targeted Early Help Assessment

- Difficulty engaging parents with services
- Struggling to provide adequate care
- Previously looked after by Local Authority
- Professionals have serious concerns e.g. parental drug/alcohol misuse, learning difficulties/mental health etc.
- Serious concerns re extremist viewpoint of parents

Level 4

Acute / Specialist Careline

- Unable to provide "good enough" parent that is adequate and safe including unbx child
- Mental health problems/substance misuse significantly affects care of child
- Parents unable to care for previous child
- Parents support and encourage extremist ideology

Ensuring Safety

- Protects from danger or significant harm in the home and elsewhere
- Restricts/monitors internet access

- Some exposure to dangerous situations in the home or community including on-line violent and/or extremist web sites or influencers
- Parental stresses starting to affect ability to ensure child's safety

- Perceived to be a problem by parents
- May be subject to neglect
- Experiencing unsafe situations
- Parents hold extremist views and condone behaviours

- Instability/violence in the home continua
- Parents involved in crime
- Parents unable to keep child safe
- Victim of crime
- Travel to areas of conflict
- Engagement with extremist activity
- Subject to traditional unsafe practices (F Force Marriage, HBV)

Emotional Warmth

- Shows warm regard, praise and encouragement

- Inconsistent responses to child by parent(s)
- Able to develop other positive relationships
- Feelings of worthlessness

- Receives erratic or inconsistent care
- Has episodes of poor quality of care
- Instability affects capacity to nurture
- Has no other positive relationships

- Parents inconsistent, highly critical or ap. towards child

Stimulation

- Facilitates cognitive development through interaction and play
- Enables child to experience success

- Spends considerable time alone e.g. watching television/computer games
- Child is not often exposed to new experiences
- Child is exposed to extremist views or organisations

- Not receiving positive stimulation, with lack of new experiences or activities
- Deliberate restricting access to positive activities and experiences
- Parents fail to challenge extremist viewpoint advocating violence

- No constructive leisure time or guided play
- Encourage to view / promote extremist ideology
- Positively denying access to positive activities and experiences

Guidance and Boundaries

- Provides guidance so that child can develop an appropriate internal model of values and conscience

- Can behave in an anti-social way in the neighbourhood e.g. petty crime
- Parent/carer offers inconsistent boundaries
- Parents offering a distorted perspective of expected boundaries
- Parents fail to challenge extremist viewpoint

- Erratic/inadequate guidance provided
- Parent not offering good role model e.g. behaving in an anti-social way
- Parents enforcing unrealistic boundaries and guidance
- No restrictions imposed re access to extreme sites/groups

- No effective boundaries set
- Regularly behaves in an anti-social way in neighbourhood
- Exposure to extremist influences
- Exhibiting behaviours to manage unrealistic negative boundaries

Stability

- Ensures that secure attachments are not disrupted
- Consistency of emotional warmth over time
- Ensures child accesses education available to them

- Key relationships with family members not always maintained
- Starting to demonstrate difficulties with attachments
- Unstable family environment

- Has multiple carers
- Has been looked after by Local Authority
- Limited attachments that are controlled by parents
- Family relationships impose negative influence

- Beyond parental control
- Has no-one to care for child
- Concerns regarding family travel to areas of conflict
- Engagement in extremist activity
- Relationships and attachments based on

C. Family and Environmental Factors

Level 1

Universal

Family History or Functioning

- Good relationships within family, even when parents are separated
- Few significant changes in family composition

Level 2

Additional Needs Multi Agency Early Help Assessment

- Parents have some conflicts or difficulties that can involve the children
- Has experienced loss of significant adult e.g. through bereavement or separation
- Looked after by younger sibling
- Parent has physical or mental health issues
- Multiple changes of address
- History of abuse
- Parents ability to cope with needs of disabled child
- Family history of criminal gang involvement, FGM, Force Marriage or HBV
- Child to adult abuse
- Extended family live in areas of conflict
- Family Religious/cultural beliefs affect role and responsibilities of child

Level 3

Complex Targeted Early Help Assessment

- Incidents of domestic violence between parents
- Acrimonious divorce/separation
- Family have serious physical and mental health difficulties
- Family associated with extremist group / ideology

Level 4

Acute / Specialist Careline

- Significant parental discord and persisters domestic violence
- Poor relationships between siblings
- Family member has Terrorism conviction
- Family Member is known to be a significance to children
- Parents negative cultural, religious beliefs practices

Wider Family

- Sense of larger familial network / good friendships outside of the family unit

- Some support from friends and family
- Caring responsibilities
- Child depressed, alone, anxious or feeling unhappy/misunderstood

- Family has poor relationship with extended family/little communication
- Caring responsibilities with no agency support
- Parents influenced by negative family, community, cultural, religious beliefs and practices
- Access to extremist networks
- Over identification with group/ideology

- No effective support from extended family
- Destructive/unhelpful involvement from extended family
- Intention to travel to area of conflict
- Engagement in terrorist activity
- Parents unable to protect from negative, manipulative influences

Housing

- Has basic amenities and appropriate facilities

- Adequate/poor housing
- Living in gang neighbourhood
- Living in an area where extremist groups (violent/non violent) operate

- Poor state of repair, temporary or overcrowded
- Homeless, living in Hostel
- Exposure to victimisation/racism
- Known extremism in wider family

- Physical accommodation places child in c

Employment

- Parents able to manage working/unemployed and do not perceive them as unduly stressful

- Periods of unemployment of the wage earning parent(s)
- Parents have limited formal education
- Parents starting to feel stressed around unemployment or working situation
- Barriers to employment opportunities

- Parents experience stress due to unemployment or "overworking"
- Parents find it difficult to obtain employment due to poor/basic skills
- Grievance resulting from inability to obtain employment

- Chronic unemployment, severely affecting parent's own identity
- Unable to gain employment due to lack of skills or long-term difficulties e.g. substance misuse

Income

- Reasonable income over time, resources used appropriately to meet needs

- Low income

- Serious debts/poverty impact on ability to meet basic needs

- Extreme poverty/debt impacting on ability care for child

Family Social Integration

- Family integrated into community
- Good social and friendship networks

- Family may be new to the area
- Some social exclusion experiences
- Negative influences from peer groups or friends
- Marginalised from community

- Parents socially excluded
- Lack of support networks
- Associating with young people who are sexually exploited
- Negative support networks
- Association with extremist groups

- Family chronically socially excluded
- No supportive network
- Family Members associated with extremist views
- Family coerced into acts of abuse

Community Resources

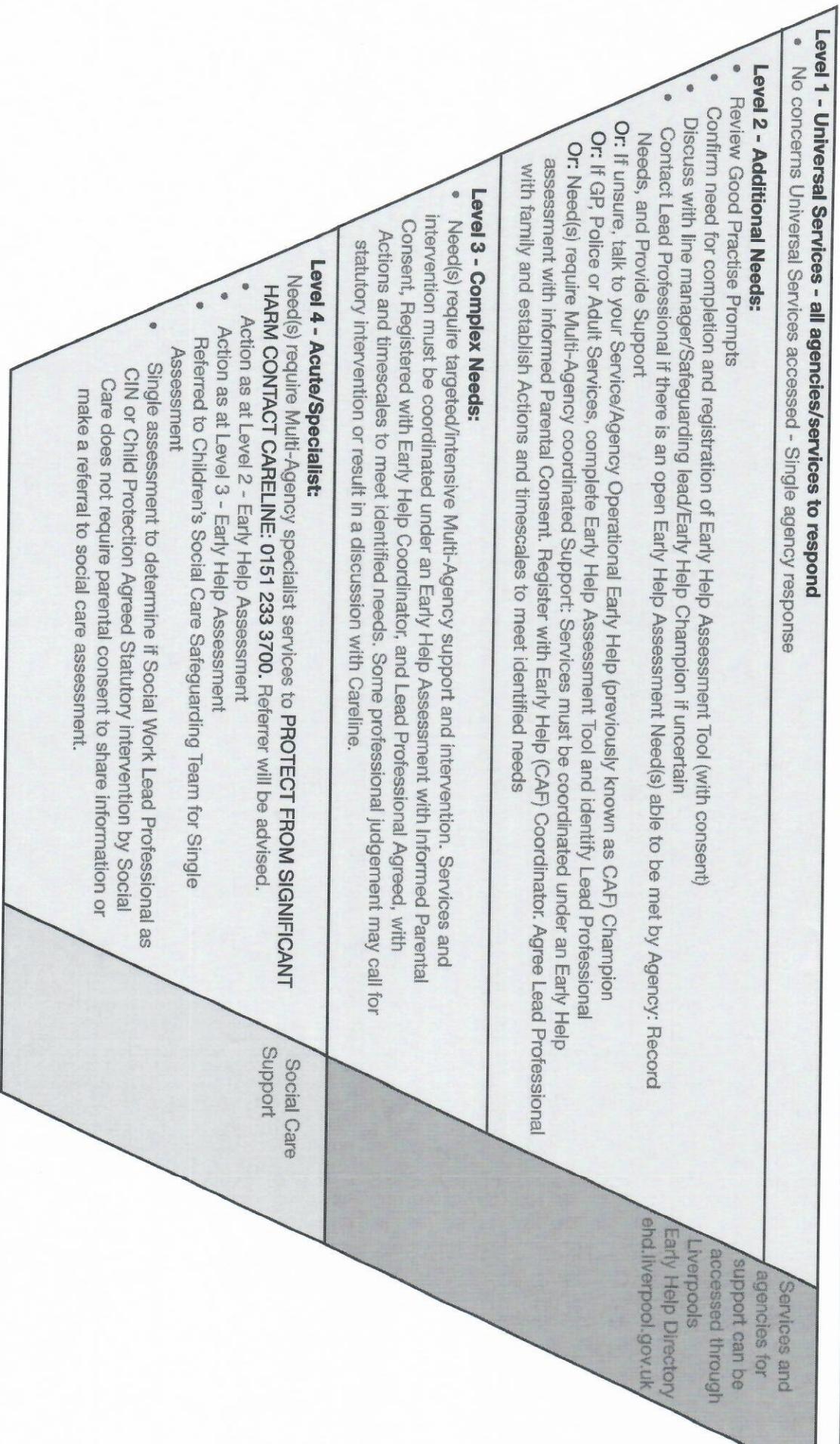
- Good universal services in neighbourhood

- Adequate universal resources but family may have access issues

- Poor quality universal resources and access problems to these and targeted

- Poor quality services with long-term difficulty with accessing target populations

Liverpool's Route to Support



Children may have needs at more than one level and may move between levels (step up/step down)

Careline: 0151 233 3700 Early Help Hub North: 0151 233 3637 Early Help Hub Central: 0151 233 6152 Early Help Hub South: 0151 233 4447

This guidance provides the general rules for most circumstances. However, all actions and decisions must be informed by professional judgement and the need to ensure the best outcomes for a child.

An Early Help Assessment Tool* must be completed where needs have been identified that require Agency /Services to support that need. Check first if one is already registered and open with the Early Help (formerly CAF) Coordinator.

To check if an Early Help Assessment is already 'open', please contact your nearest Early Help Hub:

North: T: 0151 233 3637 E: EHLHN@liverpool.gcsx.gov.uk
Central: T: 0151 233 6152 E: EHLHC@liverpool.gcsx.gov.uk
South: T: 0151 233 4447 E: EHLHS@liverpool.gcsx.gov.uk

If one is open you will be advised how to contact the lead professional. If one is not open you will be given a EHAT number to register the assessment.

IF THERE IS AN IMMEDIATE AND/OR SIGNIFICANT RISK TO A CHILD, A REFERRAL SHOULD ALWAYS BE MADE TO CARELINE. IT IS A REQUIREMENT THAT ALL REFERRALS TO CARELINE SHOULD BE THROUGH USE OF THE MARF. ONLY S47 REFERRALS SHOULD BE MADE BY TELEPHONE, AND THEN FOLLOWED UP WITH A MARF WITHIN 24 HOURS. THE MARF IS AVAILABLE AT

IF YOU BELIEVE A CRIME HAS BEEN COMMITTED, THE POLICE SHOULD ALSO BE INFORMED. TEL: 709 6010

Social Work Teams are specialist or acute services, providing assessment, planning, review and monitoring for children whose needs are complex/acute and at risk of family breakdown. These teams will carry out a Single assessment (replaces Initial and Core Assessment), and investigations under Sec 47, The Children Act 1989. They provide services at level 4 and sometimes at level 3 where the Single Assessment has confirmed Child in Need Status (Sec 17).

If you know a case is open to Social Care, contact the relevant social work team directly. If you are not sure, contact Careline (233 3700). A referral into Social Care will be via Careline, which is the first point of contact for all initial referrals. A decision will be made about whether the request for the service/referral meets the criteria for statutory services at Level 3-4. This decision must be made within 24 hours of the request for a service/referral. Careline will inform the referrer of the outcome and will also be the contact point for the team who are dealing with the referral. If a request for a service or a referral does not meet the criteria for social care involvement you will be advised accordingly. Where the request does not meet the criteria for statutory intervention, you should undertake an Assessment of need using the Early Help Assessment Tool (EHAT).

*or Early Help Pre-Assessment Tool for Police GPs and Adult Services

When making a referral, Careline will require:

- full details about the child and their circumstances
- clear details on what concerns you have about the child
- whether or not the family are aware that you have contacted Careline
- a multi-agency referral form following the conversation – accessed through LSCB/Careline website
- your availability to undertake a joint visit to the family with a Social Worker if required

Callers should expect the following from Careline:

- whether or not a referral will be accepted based on a clear rationale from the levels of need
- if accepted, the referral will be passed to the relevant team for a further discussion on appropriate action
- a Single Assessment will be undertaken by a social worker and you will be asked to contribute to this assessment and then advised of the outcome
- advised to undertake Early Help Assessment, and this will be recorded so that any follow up support can be provided where needed.

Good Practice Prompts

Information from Serious Case Reviews continues to highlight that when faced with the complex circumstances of a child's life, professionals find it difficult to keep the focus on the child and the key elements which should contribute to his or her safety.

Professionals should regularly consider these questions as a good practice prompts:

- ✓ have you been able to speak to the Child alone? Can you still do so?
- ✓ is the child at immediate risk of harm (Physical, Sexual, Neglect and Emotional)?
- ✓ is there further information you have about the child and their family? (Lack of information should not stop you making a referral, if you consider a child to be at risk)
- ✓ are there other children (siblings, peers) who could be at risk from harm?
- ✓ is there a parent or carer at risk of harm ? Do the parent or carer and the children have a safety plan?
- ✓ is it safe to discuss your concerns with the child's parents or will doing so put the child at greater risk of harm?
- ✓ is there a reason that makes it likely that the child will resist efforts to safeguard him/her (eg need for drugs)?
- ✓ have you recorded everything that has been said to you by the child?
- ✓ have you recorded everything that has been said by the parent/ family and other professionals?
- ✓ have you recorded everything that you have said to others?
- ✓ have you made every effort to engage parent/carer in agreeing to receive support, and gained consent to share information?
- ✓ have you discussed (escalated) your concerns with your agency nominated Safeguarding Children Lead ? If not, have you been able to reflect on your concerns with a colleague (in your agency or another agency) ? If you are unable to speak to your Safeguarding Lead, advice can be sought through your agency Early Help Champion or Careline Social Workers.
- ✓ have you complied with your agency's child protection procedures?
- ✓ is there a need to inform the police because a crime may have been committed?
- ✓ if consent for a referral is not provided, advice can still be requested from Careline Social Workers on a hypothetical basis.

Useful Links

All definitions used in this document have been taken from Working Together 2013

Early Help Assessment:

<http://liverpool.gov.uk/EHAT>

LSCB:

<http://liverpoolscb.org/>

Children's Service Procedures:

<http://liverpoolchildcare.proceduresonline.com/>

Working Together 2015:

<https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>

Liverpool Early Help Directory:

ehd.liverpool.gov.uk

Prevent Duty Guidance:

<https://www.gov.uk/government/publications/prevent-duty-guidance>

Child Sexual Exploitation and Children Missing from Home, Care or Education: Ofsted Targeted Inspection Guidance:

<https://www.gov.uk/government/publications/ofsted-inspections-child-sexual-exploitation-and-missing-children>

Knife, Gun and Gang Crime:

<https://www.gov.uk/government/policies/knife-gun-and-gang-crime>

Female Genital Mutilation:

<https://www.gov.uk/search?q=Female+Genital+Mutilation>



HM Government

Working Together to Safeguard Children

**A guide to inter-agency working to
safeguard and promote the welfare of
children**

July 2018

Contents

Introduction	5
About this guidance	6
What is the status of this guidance?	6
Who is this guidance for?	8
A child-centred approach to safeguarding	8
A co-ordinated approach – safeguarding is everyone’s responsibility	10
Chapter 1: Assessing need and providing help	12
Early help	12
Identifying children and families who would benefit from early help	12
Effective assessment of the need for early help.	13
Provision of effective early help services	14
Accessing help and services	15
Referral	16
Information sharing	17
Statutory requirements for children in need	20
Assessment of disabled children and their carers	21
Assessment of young carers	21
Assessment of children in secure youth establishments	21
Contextual safeguarding	22
Purpose of assessment	23
Local protocols for assessment	23
The principles and parameters of a good assessment	24
Focusing on the needs and views of the child	27
Developing a clear analysis	28
Focusing on outcomes	29
Timeliness	30
Processes for managing individual cases	31
Assessment of a child under the Children Act 1989	35
Strategy discussion	38
Initiating section 47 enquiries	42
Outcome of section 47 enquiries	44

Initial child protection conferences	46
The child protection plan	48
Child protection review conference	50
Discontinuing the Child Protection Plan	52
Chapter 2: Organisational responsibilities	55
Section 11 of the Children Act 2004	55
People in positions of trust	57
Individual organisational responsibilities	58
Schools, colleges and other educational providers	58
Early Years and Childcare	59
Health	60
Designated health professionals	61
Public Health England	62
Police	62
Adult social care services	63
Housing services	64
British Transport Police	64
Prison Service	65
Probation Service	66
Children's homes	67
The secure estate for children	67
Youth Offending Teams	68
UK Visas and Immigration, Immigration Enforcement and the Border Force	68
Children and Family Court Advisory and Support Service	69
Armed Services	69
Multi-Agency Public Protection Arrangements	70
Voluntary, charity, social enterprise, faith-based organisations and private sectors	70
Sports Clubs / Organisations	71
Chapter 3: Multi-agency safeguarding arrangements	72
Safeguarding partners	72
Leadership	73
Geographical area	74

Relevant agencies	75
Schools, colleges and other educational providers	76
Information requests	76
Independent scrutiny	77
Funding	78
Publication of arrangements	78
Dispute resolution	79
Reporting	79
Chapter 4: Improving child protection and safeguarding practice	81
Overview	81
Purpose of child safeguarding practice reviews	81
Responsibilities for reviews	82
Duty on local authorities to notify incidents to the Child Safeguarding Practice Review Panel	83
Decisions on local and national reviews	83
The rapid review	85
Guidance for the national Child Safeguarding Practice Review Panel	86
Commissioning a reviewer or reviewers for a local child safeguarding practice review	88
Local child safeguarding practice reviews	88
Expectations for the final report	89
Actions in response to local and national reviews	90
Guidance for the Child Safeguarding Practice Review Panel – reviewers	91
The Panel – expectations for the final report	91
Chapter 5: Child death reviews	93
Statutory Requirements	94
Responsibilities of Child Death Review Partners	95
Responsibilities of other organisations and agencies	96
Responding to the death of a child: the child death review process	98
Appendix A: Glossary	102
Appendix B: Further sources of information	107

Introduction

Nothing is more important than children's welfare. Children¹ who need help and protection deserve high quality and effective support as soon as a need is identified.

We want a system that responds to the needs and interests of children and families and not the other way around. In such a system, practitioners² will be clear about what is required of them individually, and how they need to work together in partnership with others.

Whilst it is parents and carers who have primary care for their children, local authorities, working with partner organisations and agencies, have specific duties to safeguard and promote the welfare of all children in their area. The Children Acts of 1989 and 2004 set out specific duties: section 17 of the Children Act 1989 puts a duty on the local authority to provide services to children in need in their area, regardless of where they are found; section 47 of the same Act requires local authorities to undertake enquiries if they believe a child has suffered or is likely to suffer significant harm. The Director of Children's Services and Lead Member for Children's Services in local authorities are the key points of professional and political accountability, with responsibility for the effective delivery of these functions.

These duties placed on the local authority can only be discharged with the full co-operation of other partners, many of whom have individual duties when carrying out their functions under section 11 of the Children Act 2004 (see chapter 2). Under section 10 of the same Act, the local authority is under a duty to make arrangements to promote co-operation between itself and organisations and agencies to improve the wellbeing of local children (see chapter 1). This co-operation should exist and be effective at all levels of an organisation, from strategic level through to operational delivery.

The Children Act 2004, as amended by the Children and Social Work Act 2017, strengthens this already important relationship by placing new duties on key agencies in a local area. Specifically the police, clinical commissioning groups and the local authority are under a duty to make arrangements to work together, and with other partners locally, to safeguard and promote the welfare of all children in their area.

Everyone who comes into contact with children and families has a role to play.

Safeguarding and promoting the welfare of children is defined for the purposes of this guidance as:

¹ In this document, a child is defined as anyone who has not yet reached their 18th birthday. 'Children' therefore means 'children and young people' throughout.

² The term 'practitioners' is used throughout the guidance to refer to individuals who work with children and their families in any capacity.

- protecting children from maltreatment
- preventing impairment of children's health or development
- ensuring that children grow up in circumstances consistent with the provision of safe and effective care
- taking action to enable all children to have the best outcomes

About this guidance

1. This guidance covers:
 - the legislative requirements placed on individual services
 - a framework for the three local safeguarding partners (the local authority; a clinical commissioning group for an area, any part of which falls within the local authority; and the chief officer of police for a police area, any part of which falls within the local authority area) to make arrangements to work together to safeguard and promote the welfare of local children including identifying and responding to their needs
 - the framework for the two child death review partners (the local authority and any clinical commissioning group for an area, any part of which falls within the local authority) to make arrangements to review all deaths of children normally resident in the local area, and if they consider it appropriate, for those not normally resident in the area
2. This document replaces Working Together to Safeguard Children (2015). Links to relevant supplementary guidance that practitioners should consider alongside this guidance can be found at Appendix B.

What is the status of this guidance?

3. This guidance applies to all organisations and agencies who have functions relating to children. Specifically, this guidance applies to all local authorities, clinical commissioning groups, police and all other organisations and agencies as set out in chapter 2.
4. It applies, in its entirety, to all schools.
5. It applies to all children up to the age of 18 years whether living with their families, in state care, or living independently.
6. This document should be complied with unless exceptional circumstances arise.

7. The guidance is issued under:
- section 7 of the Local Authority Social Services Act 1970, which requires local authorities in their social services functions to act under the general guidance of the Secretary of State
 - section 10(8) of the Children Act 2004, which requires each person or organisation to which the section 10 duty applies to have regard to any guidance given to them by the Secretary of State
 - section 11(4) of the Children Act 2004 which requires each person or organisation to which the section 11 duty applies to have regard to any guidance given to them by the Secretary of State
 - section 16B(7) of the Children Act 2004, as amended by the Children and Social Work Act 2017, which states that the Child Safeguarding Practice Review Panel must have regard to any guidance given by the Secretary of State in connection with its functions
 - section 16C(2) of the Children Act 2004, as amended by the Children and Social Work Act 2017, which states that local authorities must have regard to any guidance given by the Secretary of State in connection with their functions relating to notifications
 - section 16K of the Children Act 2004, as amended by the Children and Social Work Act 2017, which states that the safeguarding partners and relevant agencies for a local authority area in England must have regard to any guidance given by the Secretary of State in connection with their functions under sections 16E-16J of the Act
 - section 16Q of the Children Act 2004, as amended by the Children and Social Work Act 2017, which states that the child death review partners for a local authority area in England must have regard to any guidance given by the Secretary of State in connection with their functions under sections 16M-16P of the Act
 - section 175(4) of the Education Act 2002, which states that governing bodies of maintained schools (including maintained nursery schools), further education institutions and management committees of pupil referral units must have regard to any guidance given by the Secretary of State
 - paragraph 7(b) of the Schedule to the Education (Independent School Standards) Regulations 2014, made under sections 94(1) and (2) of the Education and Skills Act 2008, which states that the arrangements to safeguard or promote the welfare of pupils made by the proprietors of independent schools (including academies or free schools) or alternative provision academies must have regard to any guidance given by the Secretary of State

- paragraph 3 of the Schedule to the Non-Maintained Special Schools (England) Regulations 2015, made under section 342 of the Education Act 1996, which requires arrangements for safeguarding and promoting the health, safety and welfare of pupils in non-maintained special schools to have regard to any guidance published on such issues

Who is this guidance for?

8. This statutory guidance should be read and followed by strategic and senior leaders and frontline practitioners of all organisations and agencies as set out in chapter 2 of this document. At a strategic level, this includes local authority Chief Executives, Directors of Children's Services, chief officers of police and clinical commissioning groups and other senior leaders within organisations and agencies that commission and provide services for children and families. Members of the Child Safeguarding Practice Review Panel (see chapter 4) should also read and follow this guidance.

9. This guidance focuses on the core legal requirements, making it clear what individuals, organisations and agencies must and should do to keep children safe. In doing so, it seeks to emphasise that effective safeguarding is achieved by putting children at the centre of the system and by every individual and agency playing their full part.

A child-centred approach to safeguarding

10. This child centred approach is fundamental to safeguarding and promoting the welfare of every child. A child centred approach means keeping the child in focus when making decisions about their lives and working in partnership with them and their families.

11. All practitioners should follow the principles of the Children Acts 1989 and 2004 - that state that the welfare of children is paramount and that they are best looked after within their families, with their parents playing a full part in their lives, unless compulsory intervention in family life is necessary.

12. Children may be vulnerable to neglect and abuse or exploitation from within their family and from individuals they come across in their day-to-day lives. These threats can take a variety of different forms, including: sexual, physical and emotional abuse; neglect; exploitation by criminal gangs and organised crime groups; trafficking; online abuse; sexual exploitation and the influences of extremism leading to radicalisation. Whatever the form of abuse or neglect, practitioners should put the needs of children first when determining what action to take.

13. Children are clear about what they want from an effective safeguarding system. These asks from children should guide the behaviour of practitioners.

Children have said that they need

- vigilance: to have adults notice when things are troubling them
- understanding and action: to understand what is happening; to be heard and understood; and to have that understanding acted upon
- stability: to be able to develop an ongoing stable relationship of trust with those helping them
- respect: to be treated with the expectation that they are competent rather than not
- information and engagement: to be informed about and involved in procedures, decisions, concerns and plans
- explanation: to be informed of the outcome of assessments and decisions and reasons when their views have not met with a positive response
- support: to be provided with support in their own right as well as a member of their family
- advocacy: to be provided with advocacy to assist them in putting forward their views
- protection: to be protected against all forms of abuse and discrimination and the right to special protection and help if a refugee

14. Anyone working with children should see and speak to the child; listen to what they say; take their views seriously; and work with them and their families collaboratively when deciding how to support their needs. Special provision should be put in place to support dialogue with children who have communication difficulties, unaccompanied children, refugees and those children who are victims of modern slavery and/or trafficking. This child-centred approach is supported by:

- the Children Act 1989. This Act requires local authorities to give due regard to a child's wishes when determining what services to provide under section 17 and before making decisions about action to be taken to protect individual children under section 47. These duties complement requirements relating to the wishes and feelings of children who are, or may be, looked-after (section 22(4)), including those who are provided with accommodation under section 20 and children taken into police protection (section 46(3)(d))

- the Equality Act 2010, which puts a responsibility on public authorities to have due regard to the need to eliminate discrimination and promote equality of opportunity. This applies to the process of identification of need and risk faced by the individual child and the process of assessment. No child or group of children must be treated any less favourably than others in being able to access effective services which meet their particular needs
- the United Nations Convention on the Rights of the Child (UNCRC)³. This is an international agreement that protects the rights of children and provides a child-centred framework for the development of services to children. The UK Government ratified the UNCRC in 1991 and, by doing so, recognises children's rights to expression and receiving information

15. In addition to practitioners shaping support around the needs of individual children, local organisations and agencies should have a clear understanding of the collective needs of children locally when commissioning effective services. As part of that process, the Director of Public Health should ensure that the needs of children are a key part of the Joint Strategic Needs Assessment (JSNA) developed by the Health and wellbeing board. Safeguarding partners should use this assessment to help them understand the prevalence and contexts of need, including specific needs relating to disabled children and those relating to abuse and neglect, which in turn should help shape services.

A co-ordinated approach – safeguarding is everyone's responsibility

16. Everyone who works with children has a responsibility for keeping them safe. No single practitioner can have a full picture of a child's needs and circumstances and, if children and families are to receive the right help at the right time, everyone who comes into contact with them has a role to play in identifying concerns, sharing information and taking prompt action.

17. In order that organisations, agencies and practitioners collaborate effectively, it is vital that everyone working with children and families, including those who work with parents/carers, understands the role they should play and the role of other practitioners. They should be aware of, and comply with, the published arrangements set out by the local safeguarding partners.

18. This statutory guidance sets out key roles for individual organisations and agencies to deliver effective arrangements for safeguarding. It is essential that these arrangements are strongly led and promoted at a local level, specifically by local area leaders, including local authority Chief Executives and Lead Members of Children's Services, Mayors, the

³ [United Nations Convention on the Rights of the Child](#)

Police and Crime Commissioner and through the commitment of chief officers in all organisations and agencies, in particular those representing the three safeguarding partners. These are Directors of Children’s Services, Chief Constables of police and Accountable Officers and/or Chief Nurses of clinical commissioning groups.

19. The local authority and its social workers have specific roles and responsibilities to lead the statutory assessment of children in need (section 17, Children Act 1989) and to lead child protection enquiries (section 47, Children Act 1989). It is crucial that social workers are supported through effective supervision arrangements by practice leaders⁴ and practice supervisors, as defined under the National Assessment and Accreditation system, who have the lead role in overseeing the quality of social work practice. Designated Principal Social Workers have a key role in developing the practice and the practice methodology that underpins direct work with children and families.

⁴ Practice leaders as defined by the relevant knowledge and skills statement issued by the DfE have a key role to ensure that decisions about children are made according to this guidance.

Chapter 1: Assessing need and providing help

Early help

1. Providing early help is more effective in promoting the welfare of children than reacting later. Early help means providing support as soon as a problem emerges, at any point in a child's life, from the foundation years through to the teenage years. Early help can also prevent further problems arising; for example, if it is provided as part of a support plan where a child has returned home to their family from care, or in families where there are emerging parental mental health issues or drug and alcohol misuse.
2. Effective early help relies upon local organisations and agencies working together to:
 - identify children and families who would benefit from early help
 - undertake an assessment of the need for early help
 - provide targeted early help services to address the assessed needs of a child and their family which focuses on activity to improve the outcomes for the child
3. Local authorities, under section 10 of the Children Act 2004⁵, have a responsibility to promote inter-agency co-operation to improve the welfare of all children.

Identifying children and families who would benefit from early help

4. Local organisations and agencies should have in place effective ways to identify emerging problems and potential unmet needs of individual children and families. Local authorities should work with organisations and agencies to develop joined-up early help services based on a clear understanding of local needs. This requires all practitioners, including those in universal services and those providing services to adults with children, to understand their role in identifying emerging problems and to share information with other practitioners to support early identification and assessment.
5. Multi-agency training will be important in supporting this collective understanding of local need. Practitioners working in both universal services and specialist services have a responsibility to identify the symptoms and triggers of abuse and neglect, to share that information and provide children with the help they need. To be effective, practitioners need to continue to develop their knowledge and skills in this area and be aware of the

⁵ Section 10 of the Children Act 2004 requires each local authority to make arrangements to promote co-operation between the authority, each of the authority's relevant partners and such other persons or bodies working with children in the local authority's area as the authority considers appropriate.

new and emerging threats, including online abuse, grooming, sexual exploitation and radicalisation. To enable this, the three safeguarding partners should consider what training is needed locally and how they will monitor and evaluate the effectiveness of any training they commission.

6. Practitioners should, in particular, be alert to the potential need for early help for a child who:

- is disabled and has specific additional needs⁶
- has special educational needs (whether or not they have a statutory Education, Health and Care Plan)
- is a young carer
- is showing signs of being drawn into anti-social or criminal behaviour, including gang involvement and association with organised crime groups
- is frequently missing/goes missing from care or from home⁷
- is at risk of modern slavery, trafficking or exploitation
- is at risk of being radicalised or exploited
- is in a family circumstance presenting challenges for the child, such as drug and alcohol misuse, adult mental health issues and domestic abuse
- is misusing drugs or alcohol themselves
- has returned home to their family from care⁸
- is a privately fostered child⁹

Effective assessment of the need for early help.

7. Children and families may need support from a wide range of local organisations and agencies. Where a child and family would benefit from co-ordinated support from more than one organisation or agency (e.g. education, health, housing, police) there should be an inter-agency assessment. These early help assessments should be evidence-based, be clear about the action to be taken and services to be provided and

⁶ [Part 3 of the Children and Families Act 2014](#) promotes the physical, mental health and emotional wellbeing of children and young people with special educational needs or disabilities

⁷ [Children who run away or go missing from care \(2014\)](#)

⁸ Children return home to their families from local authority care under a range of circumstances. These circumstances and the related local authority duties are set out in flow chart 6

⁹ Private fostering occurs when a child under the age of 16 (under 18, if disabled) is provided with care and accommodation by a person who is not a parent, person with parental responsibility for them or a relative in their own home. A child is not privately fostered if the person caring for and accommodating them has done so for less than 28 days and does not intend to do so for longer.

identify what help the child and family require to prevent needs escalating to a point where intervention would be needed through a statutory assessment under the Children Act 1989.

8. A lead practitioner should undertake the assessment, provide help to the child and family, act as an advocate on their behalf and co-ordinate the delivery of support services. A GP, family support worker, school nurse, teacher, health visitor and/or special educational needs co-ordinator could undertake the lead practitioner role. Decisions about who should be the lead practitioner should be taken on a case-by-case basis and should be informed by the child and their family.

9. For an early help assessment to be effective:

- it should be undertaken with the agreement of the child and their parents or carers, involving the child and family as well as all the practitioners who are working with them. It should take account of the child's wishes and feelings wherever possible, their age, family circumstances and the wider community context in which they are living
- practitioners should be able to discuss concerns they may have about a child and family with a social worker in the local authority. Local authority children's social care should set out the process for how this will happen

10. In cases where consent is not given for an early help assessment, practitioners should consider how the needs of the child might be met. If at any time it is considered that the child may be a child in need, as defined in the Children Act 1989, or that the child has suffered significant harm or is likely to do so, a referral should be made immediately to local authority children's social care. This referral can be made by any practitioner.

Provision of effective early help services

11. The provision of early help services should form part of a continuum of support to respond to the different levels of need of individual children and families.

12. Local areas should have a comprehensive range of effective, evidence-based services in place to address assessed needs early. The early help on offer should draw upon any local assessment of need, including the JSNA and the latest evidence of the effectiveness of early help programmes. In addition to high quality support in universal services, specific local early help services will typically include family and parenting programmes, assistance with health issues, including mental health, responses to emerging thematic concerns in extra-familial contexts, and help for emerging problems relating to domestic abuse, drug or alcohol misuse by an adult or a child. Services may also focus on improving family functioning and building the family's own capability to solve

problems. This should be done within a structured, evidence-based framework involving regular review to ensure that real progress is being made. Some of these services may be delivered to parents but should always be evaluated to demonstrate the impact they are having on the outcomes for the child.

Accessing help and services

13. Where a child's need is relatively low level, individual services and universal services may be able to take swift action. Where there are more complex needs, help may be provided under section 17 of the Children Act 1989 (children in need). Where there are child protection concerns (reasonable cause to suspect a child is suffering or likely to suffer significant harm) local authority social care services must make enquiries and decide if any action must be taken under section 47 of the Children Act 1989.

14. It is important that there are clear criteria amongst all organisations and agencies working with children and families for taking action and providing help across this full continuum to ensure that services are commissioned effectively and that the right help is given to the child at the right time¹⁰.

15. In making their local arrangements, the safeguarding partners should agree with their relevant agencies the levels for the different types of assessment and services to be commissioned and delivered. This should include services for children who have suffered or are likely to suffer abuse and neglect whether from within the family or from external threats. This should also include services for disabled children and be aligned with the short breaks services statement¹¹.

16. The safeguarding partners should publish a threshold document, which sets out the local criteria for action in a way that is transparent, accessible and easily understood. This should include:

- the process for the early help assessment and the type and level of early help services to be provided
- the criteria, including the level of need, for when a case should be referred to local authority children's social care for assessment and for statutory services under:
 - section 17 of the Children Act 1989 (children in need)
 - section 47 of the Children Act 1989 (reasonable cause to suspect a child is suffering or likely to suffer significant harm)

¹⁰ Guidance on specific safeguarding concerns can be found in Appendix B.

¹¹ Required under the [Breaks for Carers of Disabled Children Regulations 2011](#).

- section 31 of the Children Act 1989 (care and supervision orders)
- section 20 of the Children Act 1989 (duty to accommodate a child)
- clear procedures and processes for cases relating to:
 - the abuse, neglect and exploitation of children
 - children managed within the youth secure estate
 - disabled children

Referral

17. Anyone who has concerns about a child's welfare should make a referral to local authority children's social care and should do so immediately if there is a concern that the child is suffering significant harm or is likely to do so. Practitioners who make a referral should always follow up their concerns if they are not satisfied with the response.

18. Local authority children's social care has the responsibility for clarifying the process for referrals. This includes specific arrangements for referrals in areas where there are secure youth establishments.

19. Within local authorities, children's social care should act as the principal point of contact for safeguarding concerns relating to children. As well as protocols for practitioners working with children and families, contact details should be signposted clearly so that children, parents and other family members are aware of who they can contact if they wish to make a referral, require advice and/or support.

20. When practitioners refer a child, they should include any information they have on the child's developmental needs, the capacity of the child's parents or carers to meet those needs and any external factors that may be undermining their capacity to parent. This information may be included in any assessment, including an early help assessment, which may have been carried out prior to a referral into local authority children's social care. Where an early help assessment has already been undertaken, it should be used to support a referral to local authority children's social care; however, this is not a prerequisite for making a referral.

21. If practitioners have concerns that a child may be a potential victim of modern slavery or human trafficking then a referral should be made to the National Referral Mechanism¹², as soon as possible.

¹² [National Referral Mechanism.](#)

22. Feedback should be given by local authority children's social care to the referrer on the decisions taken. Where appropriate, this feedback should include the reasons why a case may not meet the statutory threshold and offer suggestions for other sources of more suitable support. Practitioners should always follow up their concerns if they are not satisfied with the local authority children's social care response and should escalate their concerns if they remain dissatisfied.

Information sharing

23. Effective sharing of information between practitioners and local organisations and agencies is essential for early identification of need, assessment and service provision to keep children safe. Serious case reviews (SCRs¹³) have highlighted that missed opportunities to record, understand the significance of and share information in a timely manner can have severe consequences for the safety and welfare of children.

24. Practitioners should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children, whether this is when problems are first emerging, or where a child is already known to local authority children's social care (e.g. they are being supported as a child in need or have a child protection plan). Practitioners should be alert to sharing important information about any adults with whom that child has contact, which may impact the child's safety or welfare.

25. Information sharing is also essential for the identification of patterns of behaviour when a child has gone missing, when multiple children appear associated to the same context or locations of risk, or in relation to children in the secure estate where there may be multiple local authorities involved in a child's care. It will be for local safeguarding partners to consider how they will build positive relationships with other local areas to ensure that relevant information is shared in a timely and proportionate way.

26. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare, and protect the safety, of children, which must always be the paramount concern. To ensure effective safeguarding arrangements:

- all organisations and agencies should have arrangements in place that set out clearly the processes and the principles for sharing information. The arrangement should cover how information will be shared within their own organisation/agency; and with others who may be involved in a child's life
- all practitioners should not assume that someone else will pass on information that they think may be critical to keeping a child safe. If a practitioner has concerns

¹³ [Pathways to harm, pathways to protection: a triennial analysis of serious case reviews, 2011 to 2014](#)

about a child's welfare and considers that they may be a child in need or that the child has suffered or is likely to suffer significant harm, then they should share the information with local authority children's social care and/or the police. All practitioners should be particularly alert to the importance of sharing information when a child moves from one local authority into another, due to the risk that knowledge pertinent to keeping a child safe could be lost

- all practitioners should aim to gain consent to share information, but should be mindful of situations where to do so would place a child at increased risk of harm. Information may be shared without consent if a practitioner has reason to believe that there is good reason to do so, and that the sharing of information will enhance the safeguarding of a child in a timely manner. When decisions are made to share or withhold information, practitioners should record who has been given the information and why

27. Practitioners must have due regard to the relevant data protection principles which allow them to share personal information, as provided for in the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). To share information effectively:

- all practitioners should be confident of the processing conditions under the Data Protection Act 2018 and the GDPR which allow them to store and share information for safeguarding purposes, including information which is sensitive and personal, and should be treated as 'special category personal data'
- where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 contains 'safeguarding of children and individuals at risk' as a processing condition that allows practitioners to share information. This includes allowing practitioners to share information without consent, if it is not possible to gain consent, it cannot be reasonably expected that a practitioner gains consent, or if to gain consent would place a child at risk

Myth-busting guide to information sharing

Sharing information enables practitioners and agencies to identify and provide appropriate services that safeguard and promote the welfare of children. Below are common myths that may hinder effective information sharing.

Data protection legislation is a barrier to sharing information

No – the Data Protection Act 2018 and GDPR do not prohibit the collection and sharing of personal information, but rather provide a framework to ensure that personal information is shared appropriately. In particular, the Data Protection Act 2018 balances the rights of the information subject (the individual whom the information is about) and the possible need to share information about them.

Consent is always needed to share personal information

No – you do not necessarily need consent to share personal information. Wherever possible, you should seek consent and be open and honest with the individual from the outset as to why, what, how and with whom, their information will be shared. You should seek consent where an individual may not expect their information to be passed on. When you gain consent to share information, it must be explicit, and freely given. There may be some circumstances where it is not appropriate to seek consent, because the individual cannot give consent, or it is not reasonable to obtain consent, or because to gain consent would put a child's or young person's safety at risk.

Personal information collected by one organisation/agency cannot be disclosed to another

No – this is not the case, unless the information is to be used for a purpose incompatible with the purpose for which it was originally collected. In the case of children in need, or children at risk of significant harm, it is difficult to foresee circumstances where information law would be a barrier to sharing personal information with other practitioners¹⁴.

The common law duty of confidence and the Human Rights Act 1998 prevent the sharing of personal information

No – this is not the case. In addition to the Data Protection Act 2018 and GDPR, practitioners need to balance the common law duty of confidence and the Human Rights Act 1998 against the effect on individuals or others of not sharing the information.

IT Systems are often a barrier to effective information sharing

No – IT systems, such as the Child Protection Information Sharing project (CP-IS), can be useful for information sharing. IT systems are most valuable when practitioners use the shared data to make more informed decisions about how to support and safeguard a child.

¹⁴ Practitioners looking to share information should consider which processing condition in the Data Protection Act 2018 is most appropriate for use in the particular circumstances of the case. This may be the safeguarding processing condition or another relevant provision.

Statutory requirements for children in need

- under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare
- local authorities undertake assessments of the needs of individual children and must give due regard to a child's age and understanding when determining what, if any, services to provide. Every assessment must be informed by the views of the child as well as the family, and a child's wishes and feelings must be sought regarding the provision of services to be delivered. Where possible, children should be seen alone
- a child in need is defined under the Children Act 1989 as a child who is unlikely to achieve or maintain a reasonable level of health or development, or whose health and development is likely to be significantly or further impaired, without the provision of services; or a child who is disabled. Children in need may be assessed under section 17 of the Children Act 1989 by a social worker
- some children in need may require accommodation because there is no one who has parental responsibility for them, because they are lost or abandoned, or because the person who has been caring for them is prevented from providing them with suitable accommodation or care. Under section 20 of the Children Act 1989, the local authority has a duty to accommodate such children in need in their area
- when assessing children in need and providing services, specialist assessments may be required and, where possible, should be co-ordinated so that the child and family experience a coherent process and a single plan of action
- under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child (who lives or is found in their area) is suffering or is likely to suffer significant harm, it has a duty to make such enquiries as it considers necessary to decide whether to take any action to safeguard or promote the child's welfare. Such enquiries, supported by other organisations and agencies, as appropriate, should be initiated where there are concerns about all forms of abuse, neglect. This includes female genital mutilation and other honour-based violence, and extra-familial threats including radicalisation and sexual or criminal exploitation
- there may be a need for immediate protection whilst an assessment or enquiries are carried out

Assessment of disabled children and their carers

28. When undertaking an assessment of a disabled child, the local authority must also consider whether it is necessary to provide support under section 2 of the Chronically Sick and Disabled Persons Act (CSDPA) 1970¹⁵. Where a local authority is satisfied that the identified services and assistance can be provided under section 2 of the CSDPA, and it is necessary in order to meet a disabled child's needs, it must arrange to provide that support. Where a local authority is assessing the needs of a disabled child, a carer of that child may also require the local authority to undertake an assessment of their ability to provide, or to continue to provide, care for the child, under section 1 of the Carers (Recognition and Services) Act 1995. The local authority must take account of the results of any such assessment when deciding whether to provide services to the disabled child.

29. If a local authority considers that a parent carer of a disabled child (see glossary) may have support needs, it must carry out an assessment under section 17ZD of the Children Act 1989. The local authority must also carry out such an assessment if a parent carer requests one. Such an assessment must consider whether it is appropriate for the parent carer to provide, or continue to provide, care for the disabled child, in light of the parent carer's needs and wishes.

Assessment of young carers

30. If a local authority considers that a young carer (see glossary) may have support needs, it must carry out an assessment under section 17ZA of the Children Act 1989. The local authority must also carry out such an assessment if a young carer, or the parent of a young carer, requests one. Such an assessment must consider whether it is appropriate or excessive for the young carer to provide care for the person in question, in light of the young carer's needs and wishes. The Young Carers' (Needs Assessment) Regulations 2015¹⁶ require local authorities to look at the needs of the whole family when carrying out a young carer's needs assessment. Young carers' assessments can be combined with assessments of adults in the household, with the agreement of the young carer and adults concerned.

Assessment of children in secure youth establishments

31. Any assessment of children in secure youth establishments should take account of their specific needs. In all cases, the local authority in which a secure youth establishment is located is responsible for the safety and welfare of the children in that establishment. The host local authority should work with the governor, director, manager or principal of

¹⁵ [Chronically Sick and Disabled Persons Act \(CSDPA\) 1970.](#)

¹⁶ [The Young Carers' \(Need Assessment\) Regulations 2015.](#)

the secure youth establishment and the child's home local authority, their relevant Youth Offending Team and, where appropriate, the Youth Custody Service¹⁷ to ensure that the child has a single, comprehensive support plan.

32. Where a child becomes looked-after, as a result of being remanded to youth detention accommodation (YDA), the local authority must visit the child and assess the child's needs before taking a decision. This information must be used to prepare a Detention Placement Plan (DPP), which must set out how the YDA and other practitioners will meet the child's needs whilst the child remains remanded. The DPP must be reviewed in the same way as a care plan for any other looked-after child¹⁸.

Contextual safeguarding

33. As well as threats to the welfare of children from within their families, children may be vulnerable to abuse or exploitation from outside their families. These extra-familial threats might arise at school and other educational establishments, from within peer groups, or more widely from within the wider community and/or online. These threats can take a variety of different forms and children can be vulnerable to multiple threats, including: exploitation by criminal gangs and organised crime groups such as county lines; trafficking, online abuse; sexual exploitation and the influences of extremism leading to radicalisation. Extremist groups make use of the internet to radicalise and recruit and to promote extremist materials. Any potential harmful effects to individuals identified as vulnerable to extremist ideologies or being drawn into terrorism should also be considered¹⁹.

34. Assessments of children in such cases should consider whether wider environmental factors are present in a child's life and are a threat to their safety and/or welfare. Children who may be alleged perpetrators should also be assessed to understand the impact of contextual issues on their safety and welfare. Interventions should focus on addressing these wider environmental factors, which are likely to be a threat to the safety and welfare of a number of different children who may or may not be known to local authority children's social care. Assessments of children in such cases should consider the individual needs and vulnerabilities of each child. They should look at the parental capacity to support the child, including helping the parents and carers to understand any risks and support them to keep children safe and assess potential risk to child.

¹⁷ As the placing authority.

¹⁸ Following the [Legal Aid Sentencing and Punishment of Offenders Act 2012](#) all children and young people remanded by a court in criminal proceedings will be looked-after.

¹⁹ Under the [Counter-Terrorism and Security Act 2015](#).

35. Channel panels, established under the Counter-Terrorism and Security Act 2015, assess the extent to which identified individuals are vulnerable to being drawn into terrorism, and, where appropriate, arrange for support to be provided²⁰. When assessing Channel referrals, local authorities and their partners should consider how best to align these with assessments undertaken under the Children Act 1989.

36. The Children Act 1989 promotes the view that all children and their parents should be considered as individuals and that family structures, culture, religion, ethnic origins and other characteristics should be respected. Local authorities should ensure they support and promote fundamental British values, of democracy, the rule of law, individual liberty, and mutual respect and tolerance of those with different faiths and beliefs.

37. The Counter-Terrorism and Security Act 2015 contains a duty on specified authorities in England, Wales and Scotland to have due regard to the need to prevent people from being drawn into terrorism.

Purpose of assessment

38. Whatever legislation the child is assessed under, the purpose of the assessment is always:

- to gather important information about a child and family
- to analyse their needs and/or the nature and level of any risk and harm being suffered by the child
- to decide whether the child is a child in need (section 17) or is suffering or likely to suffer significant harm (section 47)
- to provide support to address those needs to improve the child's outcomes and welfare and where necessary to make them safe

Local protocols for assessment

39. Local authorities, with their partners, should develop and publish local protocols for assessment. A local protocol should set out clear arrangements for how cases will be managed once a child is referred into local authority children's social care and be consistent with the requirements of this statutory guidance. The detail of each protocol will be led by the local authority in discussion and agreement with the safeguarding partners and relevant agencies where appropriate.

²⁰ [Channel guidance](#).

40. The local authority is publicly accountable for this protocol and all organisations and agencies have a responsibility to understand their local protocol.

41. The local protocol should reflect where assessments for some children will require particular care. This is especially so for young carers, children with special educational needs (including to inform and be informed by Education, Health and Care Plans), unborn children where there are concerns, children in hospital, children with specific communication needs, asylum seeking children, children considered at risk of gang activity and association with organised crime groups, children at risk of female genital mutilation, children who are in the youth justice system, and children returning home.

42. Where a child has other assessments, it is important that these are co-ordinated so that the child does not become lost between the different organisational procedures. There should be clear procedures for how these organisations and agencies will communicate with the child and family, and the local protocol for assessment should clarify how organisations and agencies and practitioners undertaking assessments and providing services can make contributions.

43. The local protocol for assessment should set out the process for challenge by children and families by publishing the complaints procedures²¹.

The principles and parameters of a good assessment

44. Assessment should be a dynamic process, which analyses and responds to the changing nature and level of need and/or risk faced by the child from within and outside their family. It is important that the impact of what is happening to a child is clearly identified and that information is gathered, recorded and checked systematically, and discussed with the child and their parents/carers where appropriate.

45. Any provision identified as being necessary through the assessment process should, if the local authority decides to provide such services, be provided without delay. A good assessment will monitor and record the impact of any services delivered to the child and family and review the help being delivered. Whilst services may be delivered to a parent or carer, the assessment should be focused on the needs of the child and on the impact any services are having on the child²².

46. Good assessments support practitioners to understand whether a child has needs relating to their care or a disability and/or is suffering or likely to suffer significant harm.

²¹ Including as specified under [Section 26\(3\) of the Children Act 1989](#) and the [Children Act 1989 Representations Procedure \(England\) Regulations 2006](#).

²² An assessment of the support needs of parent carers, or non-parent carers, of disabled children may be required.

The specific needs of disabled children and young carers should be given sufficient recognition and priority in the assessment process²³.

47. The local authority should act decisively to protect the child from abuse and neglect including initiating care proceedings where existing interventions are insufficient²⁴. Where an assessment in these circumstances identifies concerns but care proceedings are not initiated, the assessment should provide a valuable platform for ongoing engagement with the child and their family.

48. Where a child becomes looked-after, the assessment will be the baseline for work with the family. Any needs that have been identified should be addressed before decisions are made about the child's return home. Assessment by a social worker is required before a looked after child under a care order returns home²⁵. This will provide evidence of whether the necessary improvements have been made to ensure the child's safety when they return home. Following an assessment, appropriate support should be provided for children returning home, including where that return home is unplanned, to ensure that children continue to be adequately safeguarded.

49. In order to carry out good assessments, social workers should have the relevant knowledge and skills set out in the Knowledge and Skills Statements for child and family social work²⁶.

50. Social workers should have time to complete assessments and have access to high quality practice supervision. Principal social workers should support social workers, the local authority and partners to develop their assessment practice and decision making skills, and the practice methodology that underpins this.

51. High quality assessments:

- are child-centred. Where there is a conflict of interest, decisions should be made in the child's best interests: be rooted in child development: be age-appropriate; and be informed by evidence
- are focused on action and outcomes for children
- are holistic in approach, addressing the child's needs within their family and any risks the child faces from within the wider community
- ensure equality of opportunity

²³ [Recognised, valued and supported: Next steps for the Carers Strategy \(2010\)](#).

²⁴ Further information about processes relating to care and court proceedings (including pre-proceedings) can be found in the statutory guidance document for local authorities, [Court Orders and Pre-Proceedings](#) (DfE, 2014).

²⁵ [Under the Care Planning, Placement and Case Review \(England\) Regulations 2010](#).

²⁶ [Knowledge and skills statements for child and family social work](#).

- involve children, ensuring that their voice is heard and provide appropriate support to enable this where the child has specific communication needs
- involve families
- identify risks to the safety and welfare of children
- build on strengths as well as identifying difficulties
- are integrated in approach
- are multi-agency and multi-disciplinary
- are a continuing process, not an event
- lead to action, including the provision of services
- review services provided on an ongoing basis
- are transparent and open to challenge

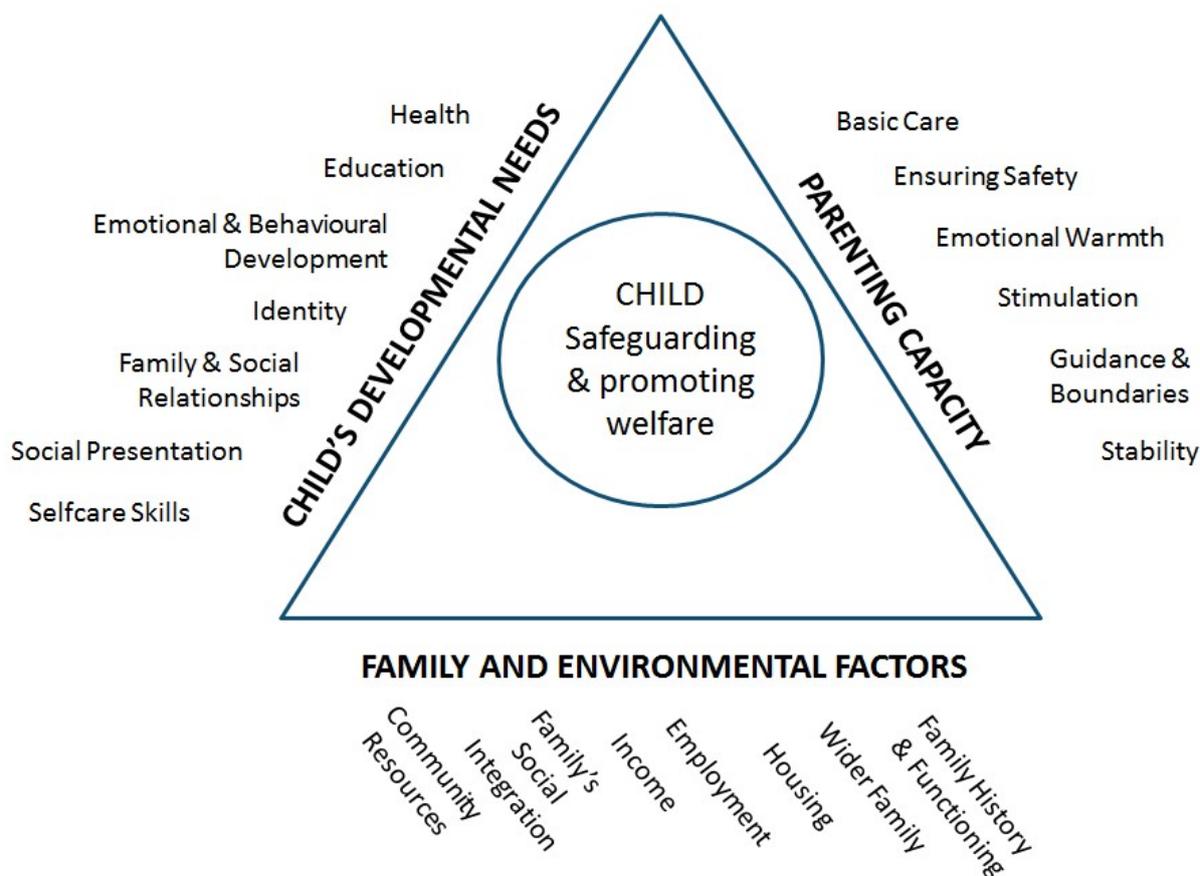
52. Research has shown that taking a systematic approach to enquiries using a conceptual model is the best way to deliver a comprehensive assessment for all children. An example of such a model is set out in the diagram on the next page. It investigates three domains:

- the child's developmental needs, including whether they are suffering or likely to suffer significant harm
- the capacity of parents or carers (resident and non-resident) and any other adults living in the household to respond to those needs ^{27, 28}
- the impact and influence of wider family and any other adults living in the household as well as community and environmental circumstances

²⁷ An assessment of the support needs of parent carers of disabled children may be required.

²⁸ See Chapter 2 paragraph 30 on adults with parental responsibility for disabled children.

Assessment Framework



Focusing on the needs and views of the child

53. Every assessment should reflect the unique characteristics of the child within their family and community context. Each child whose referral has been accepted by children's social care should have their individual needs assessed, including an analysis of the parental capacity to meet those needs whether they arise from issues within the family or the wider community. Frequently, more than one child from the same family is referred and siblings within the family should always be considered. Family assessments that include all members of the family should always ensure that the needs of individual children are distinct considerations.

54. Where the child has links to a foreign country²⁹, a social worker may also need to work with colleagues abroad³⁰.

²⁹ A child with links to a foreign country may be a foreign national child, a child with dual nationality or a British child of foreign parents/national origin.

³⁰ Further guidance can be found in [Working with foreign authorities: child protection and care orders](#) (2014).

55. Every assessment, including young carer, parent carer and non-parent carer assessments, should draw together relevant information gathered from the child and their family and from relevant practitioners including teachers and school staff, early years workers, health practitioners, the police and adult social care. Where a child has been looked-after and has returned home, information from previous assessments and case records should also be reviewed.

Developing a clear analysis

56. The social worker should analyse all the information gathered from the assessment, including from a young carer's, parent carer's or non-parent carer's assessment, to decide the nature and level of the child's needs and the level of risk, if any, they may be facing. The social worker should receive insight and challenge to their emerging hypothesis from their practice supervisors and other relevant practitioners who should challenge the social worker's assumptions as part of this process. An informed decision should be taken on the nature of any action required and which services should be provided. Social workers, their managers and other practitioners should be mindful of the requirement to understand the level of need and risk in, or faced by, a family from the child's perspective and plan accordingly, understanding both protective and risk factors the child is facing. The analysis should inform the action to be taken which will have maximum impact on the child's welfare and outcomes.

57. No system can fully eliminate risk. Understanding risk involves judgment and balance. To manage risks, social workers and other practitioners should make decisions with the best interests of the child in mind, informed by the evidence available and underpinned by knowledge of child development.

58. Critical reflection through supervision should strengthen the analysis in each assessment.

59. A desire to think the best of adults and to hope they can overcome their difficulties should not subvert the need to protect children from chaotic, abusive and neglectful homes. Social workers and practice supervisors should always reflect the latest research on the impact of abuse and neglect and relevant findings from serious case and practice reviews when analysing the level of need and risk faced by the child. This should be reflected in the case recording.

60. Assessment is a dynamic and continuous process that should build upon the history of every individual case, responding to the impact of any previous services and analysing what further action might be needed. Social workers should build on this with help from other practitioners from the moment that a need is identified. A high quality

assessment is one in which evidence is built and revised throughout the process and takes account of family history and the child's experience of cumulative abuse.

61. A social worker may arrive at a judgment early in the case but this may need to be revised as the case progresses and further information comes to light. It is a characteristic of skilled practice that social workers revisit their assumptions in the light of new evidence and take action to revise their decisions in the best interests of the individual child.

62. Decision points and review points involving the child and family and relevant practitioners should be used to keep the assessment on track. This is to ensure that help is given in a timely and appropriate way and that the impact of this help is analysed and evaluated in terms of the improved outcomes and welfare of the child.

Focusing on outcomes

63. Every assessment should be focused on outcomes, deciding which services and support to provide to deliver improved welfare for the child.

64. Where the outcome of the assessment is continued local authority children's social care involvement, the social worker should agree a plan of action with other practitioners and discuss this with the child and their family. The plan should set out what services are to be delivered, and what actions are to be undertaken, by whom and for what purpose.

65. Many services provided will be for parents or carers (and may include services identified in a parent carer's or non-parent carer's needs assessment)³¹. The plan should reflect this and set clear measurable outcomes for the child and expectations for the parents, with measurable, reviewable actions for them.

66. The plan should be reviewed regularly to analyse whether sufficient progress has been made to meet the child's needs and the level of risk faced by the child. This will be important for neglect cases where parents and carers can make small improvements. The test should be whether any improvements in adult behaviour are sufficient and sustained. Social workers should consider the need for further action and record their decisions. The review points should be agreed by the social worker with other practitioners and with the child and family to continue evaluating the impact of any change on the welfare of the child.

67. Effective practitioner supervision can play a critical role in ensuring a clear focus on a child's welfare. Supervision should support practitioners to reflect critically on the impact of their decisions on the child and their family. The social worker should review the plan for the child. They should ask whether the help given is leading to a significant positive

³¹ Section 17ZD of the Children Act 1989 and section 1 of the [Carers \(Recognition and Services\) Act 1995](#).

change for the child and whether the pace of that change is appropriate for the child. Practitioners working with children should always have access to colleagues to talk through their concerns and judgments affecting the welfare of the child. Assessment should remain an ongoing process, with the impact of services informing future decisions about action.

68. Known transition points for the child should be planned for in advance. This includes where children are likely to transition between child and adult services.

Timeliness

69. The timeliness of an assessment is a critical element of the quality of that assessment and the outcomes for the child. The speed with which an assessment is carried out after a child's case has been referred into local authority children's social care should be determined by the needs of the individual child and the nature and level of any risk of harm they face. This will require judgments to be made by the social worker on each individual case. Adult assessments, for example, parent carer or non-parent carer assessments, should also be carried out in a timely manner, consistent with the needs of the child.

70. Once the referral has been accepted by local authority children's social care, the lead practitioner role falls to a social worker. The social worker should clarify with the referrer, when known, the nature of the concerns and how and why they have arisen.

71. Within **one working day** of a referral being received, a local authority social worker should acknowledge receipt to the referrer and **make a decision** about next steps and the type of response required. This will include determining whether:

- the child requires immediate protection and urgent action is required
- the child is in need and should be assessed under section 17 of the Children Act 1989
- there is reasonable cause to suspect that the child is suffering or likely to suffer significant harm, and whether enquires must be made and the child assessed under section 47 of the Children Act 1989
- any services are required by the child and family and what type of services
- further specialist assessments are required to help the local authority to decide what further action to take
- to see the child as soon as possible if the decision is taken that the referral requires further assessment

72. Where requested to do so by local authority children's social care, practitioners from other parts of the local authority such as housing and those in health organisations have a duty to co-operate under section 27 of the Children Act 1989 by assisting the local authority in carrying out its children's social care functions.

73. The child and family must be informed of the action to be taken, unless a decision is taken on the basis that this may jeopardise a police investigation or place the child at risk of significant harm.

74. For children who are in need of immediate protection, action must be taken by the social worker, or the police or the NSPCC³² if removal is required, as soon as possible after the referral has been made to local authority children's social care (sections 44 and 46 of the Children Act 1989).

75. The maximum timeframe for the assessment to conclude, such that it is possible to reach a decision on next steps, should be no longer than 45 working days from the point of referral. If, in discussion with a child and their family and other practitioners, an assessment exceeds 45 working days, the social worker should record the reasons for exceeding the time limit.

76. Whatever the timescale for assessment, where particular needs are identified at any stage of the assessment, social workers should not wait until the assessment reaches a conclusion before commissioning services to support the child and their family. In some cases, the needs of the child will mean that a quick assessment will be required.

77. It is the responsibility of the social worker to make clear to children and families how the assessment will be carried out and when they can expect a decision on next steps. Local authorities should determine their local assessment processes through a local protocol.

Processes for managing individual cases

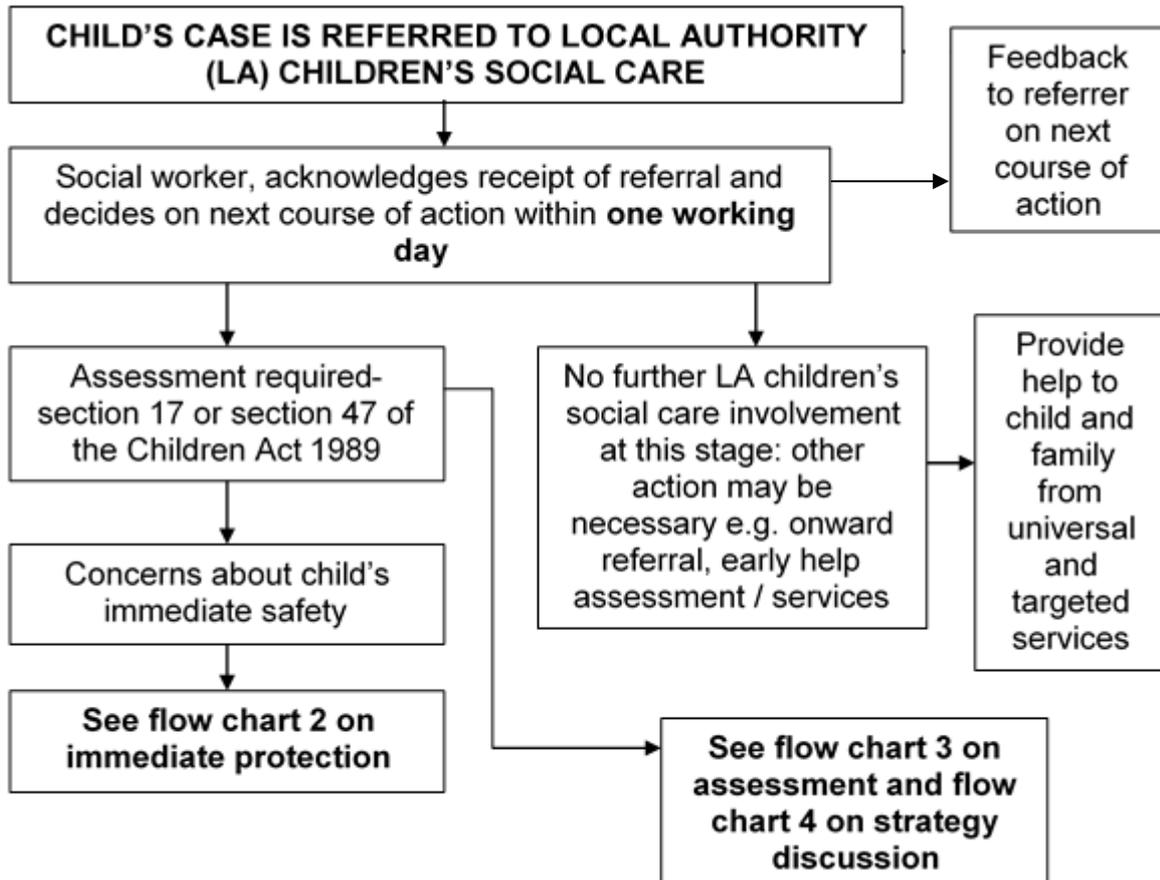
78. The following descriptors and flow charts set out the steps that practitioners should take when working together to assess and provide services for children who may be in need, including those suffering harm. The flow charts cover:

- the referral process into local authority children's social care
- immediate protection for children at risk of significant harm
- the process for determining next steps for a child who has been assessed as being 'in need'

³² [National Society for the Prevention of Cruelty to Children.](#)

- the processes for children where there is reasonable cause to suspect that the child is suffering or likely to suffer significant harm (this includes immediate protection for children at serious risk of harm)

Flow chart 1: Action taken when a child is referred to local authority children’s social care services



Immediate Protection

Where there is a risk to the life of a child or a likelihood of serious immediate harm, local authority social workers, the police or NSPCC should use their statutory child protection powers to **act immediately to secure the safety of the child**.

If it is necessary to remove a child from their home, a local authority must, wherever possible and unless a child's safety is otherwise at immediate risk, apply for an **Emergency Protection Order (EPO)**. Police powers to remove a child in an emergency should be used only in exceptional circumstances where there is insufficient time to seek an EPO or for reasons relating to the immediate safety of the child.

An **EPO**, made by the court, gives authority to remove a child and places them under the protection of the applicant.

When considering whether emergency action is necessary, an agency should always consider the needs of other children in the same household or in the household of an alleged perpetrator.

The **local authority** in whose area a child is found in circumstances that require emergency action (the first authority) is responsible for taking emergency action.

If the child is looked-after by, or the subject of a child protection plan in another authority, the first authority must consult the authority responsible for the child. Only when the second local authority explicitly accepts responsibility (to be followed up in writing) is the first authority relieved of its responsibility to take emergency action.

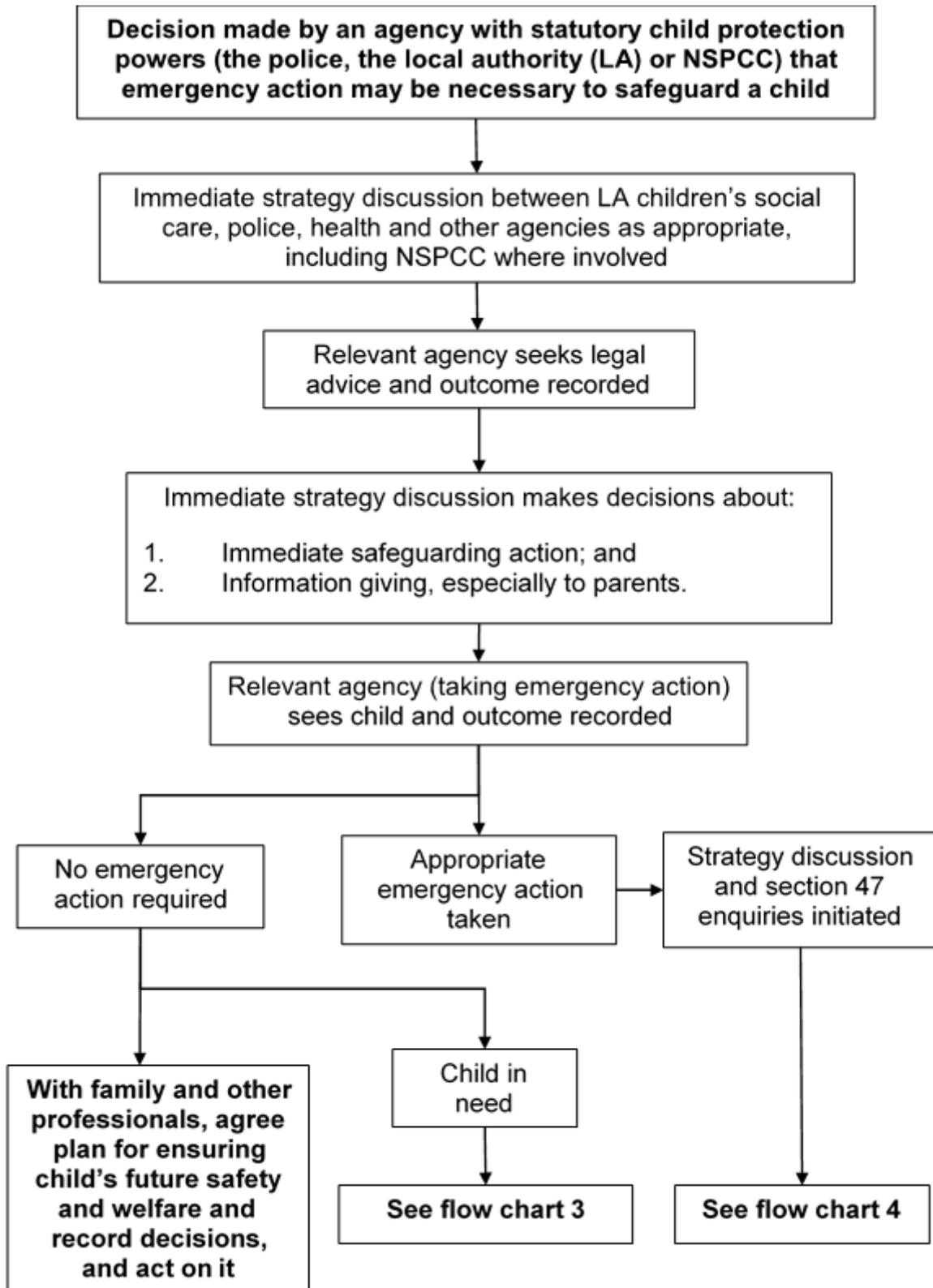
Multi-agency working

Planned emergency action will normally take place following an immediate strategy discussion. Social workers, the police or NSPCC should:

- initiate a strategy discussion to discuss planned emergency action. Where a single agency has to act immediately, a strategy discussion should take place as soon as possible after action has been taken
- see the child (this should be done by a practitioner from the agency taking the emergency action) to decide how best to protect them and whether to seek an EPO
- wherever possible, obtain legal advice before initiating legal action, in particular when an EPO is being sought

Related information: For further guidance on EPOs see Chapter 4 of *the statutory guidance document for local authorities*, [Court orders and pre-proceedings](#) (DfE, April 2014).

Flow chart 2: Immediate protection



Assessment of a child under the Children Act 1989

Following acceptance of a referral by the local authority children's social care, a social worker should lead a multi-agency assessment under section 17 of the Children Act 1989. Local authorities have a duty to ascertain the child's wishes and feelings and take account of them when planning the provision of services. Assessments should be carried out in a timely manner reflecting the needs of the individual child, as set out in this chapter.

Where the local authority children's social care decides to provide services, a multi-agency child in need plan should be developed which sets out which organisations and agencies will provide which services to the child and family. The plan should set clear measurable outcomes for the child and expectations for the parents. The plan should reflect the positive aspects of the family situation as well as the weaknesses.

Where a child in need has moved permanently to another local authority area, the original authority should ensure that all relevant information (including the child in need plan) is shared with the receiving local authority as soon as possible. The receiving local authority should consider whether support services are still required and discuss with the child and family what might be needed, based on a timely re-assessment of the child's needs, as set out in this chapter. Support should continue to be provided by the original local authority in the intervening period. The receiving authority should work with the original authority to ensure that any changes to the services and support provided are managed carefully.

Where a child in need is approaching 18 years of age, this transition point should be planned for in advance. This includes where children are likely to transition between child and adult services.

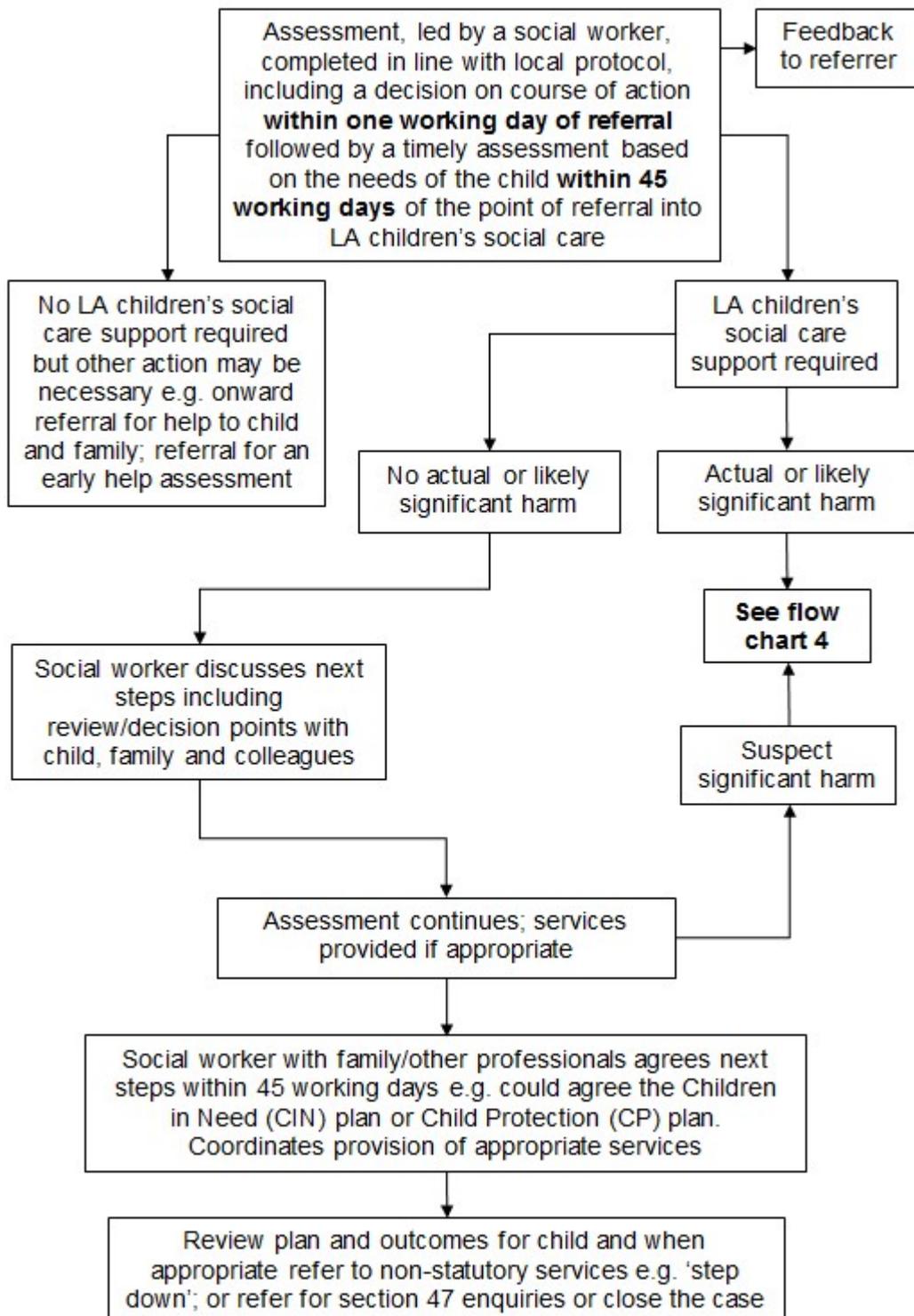
Where information gathered during an assessment (which may be very brief) results in the social worker suspecting that the child is suffering or likely to suffer significant harm, the local authority should hold a strategy discussion to enable it to decide, with other agencies, whether it must initiate enquiries under section 47 of the Children Act 1989.

Purpose:	Assessments should determine whether the child is in need, the nature of any services required and whether any specialist assessments should be undertaken to assist the local authority in its decision-making.
-----------------	--

Assessment of a child under the Children Act 1989

Social workers should:	<ul style="list-style-type: none">• lead on an assessment and complete it in line with the locally agreed protocol according to the child's needs and within 45 working days from the point of referral into local authority children's social care• see the child within a timescale that is appropriate to the nature of the concerns expressed at referral, according to an agreed plan• conduct interviews with the child and family members, separately and together as appropriate. Initial discussions with the child should be conducted in a way that minimises distress to them and maximises the likelihood that they will provide accurate and complete information, avoiding leading or suggestive questions• record the assessment findings and decisions and next steps following the assessment• inform, in writing, all the relevant agencies and the family of their decisions and, if the child is a child in need, of the plan for providing support• inform the referrer of what action has been or will be taken
The police should:	<ul style="list-style-type: none">• assist other organisations and agencies to carry out their responsibilities where there are concerns about the child's welfare, whether or not a crime has been committed. If a crime has been committed, the police should be informed by the local authority children's social care
All involved practitioners should:	<ul style="list-style-type: none">• be involved in the assessment and provide further information about the child and family• agree further action including what services would help the child and family and inform local authority children's social care if any immediate action is required• seek advice and guidance as required and in line with local practice guidance

Flow chart 3: Action taken for an assessment of a child under the Children Act 1989



Strategy discussion

Whenever there is reasonable cause to suspect that a child is suffering or is likely to suffer significant harm there should be a strategy discussion involving local authority children's social care (including the residential or fostering service, if the child is looked-after), the police, health and other bodies such as the referring agency. This might take the form of a multi-agency meeting or phone calls and more than one discussion may be necessary. A strategy discussion can take place following a referral or at any other time, including during the assessment process and when new information is received on an already open case.

Purpose:

Local authority children's social care should convene a strategy discussion to determine the child's welfare and plan rapid future action if there is reasonable cause to suspect the child is suffering or is likely to suffer significant harm.

Strategy discussion attendees:

A local authority social worker, health practitioners and a police representative should, as a minimum, be involved in the strategy discussion. Other relevant practitioners will depend on the nature of the individual case but may include:

- the practitioner or agency which made the referral
- the child's school or nursery
- any health or care services the child or family members are receiving

All attendees should be sufficiently senior to make decisions on behalf of their organisation and agencies.

Strategy discussion

Strategy discussion tasks:

The discussion should be used to:

- share available information
- agree the conduct and timing of any criminal investigation
- decide whether enquiries under section 47 of the Children Act 1989 must be undertaken

Where there are grounds to initiate an enquiry under section 47 of the Children Act 1989, decisions should be made as to:

- what further information is needed if an assessment is already underway and how it will be obtained and recorded
- what immediate and short term action is required to support the child, and who will do what by when
- whether legal action is required

The timescale for the assessment to reach a decision on next steps should be based upon the needs of the individual child, consistent with the local protocol and no longer than **45 working days** from the point of referral into local authority children's social care.

The principles and parameters for the assessment of children in need at chapter 1 paragraph 40 should be followed for assessments undertaken under section 47 of the Children Act 1989.

Social workers should:

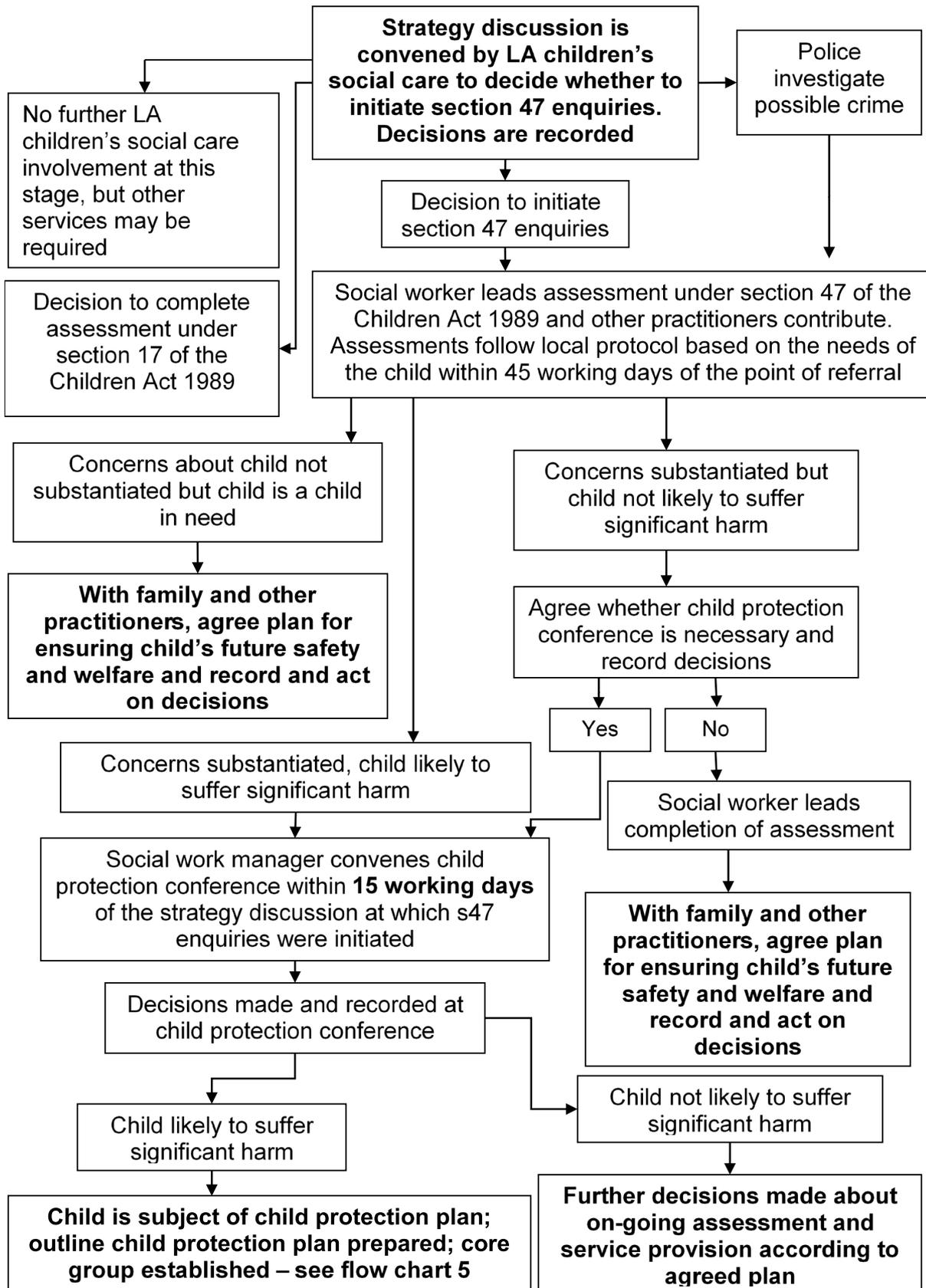
Convene the strategy discussion and make sure it:

- considers the child's welfare and safety, and identifies the level of risk faced by the child
- decides what information should be shared with the child and family (on the basis that information is not shared if this may jeopardise a police investigation or place the child at risk of significant harm)
- agrees what further action is required, and who will do what by when, where an EPO is in place or the child is the subject of police powers of protection
- records agreed decisions in accordance with local recording procedures
- follows up actions to make sure what was agreed gets done

Strategy discussion

Health practitioners should:	<ul style="list-style-type: none">• advise about the appropriateness or otherwise of medical assessments, and explain the benefits that arise from assessing previously unmanaged health matters that may be further evidence of neglect or maltreatment• provide and co-ordinate any specific information from relevant practitioners regarding family health, maternity health, school health mental health, domestic abuse and violence and substance misuse to assist strategy and decision making• secure additional expert advice and support from named and/or designated professionals for more complex cases following preliminary strategy discussions• undertake appropriate examinations or observations, and further investigations or tests, to determine how the child's health or development may be impaired
The police should:	<ul style="list-style-type: none">• discuss the basis for any criminal investigation and any relevant processes that other organisations and agencies might need to know about, including the timing and methods of evidence gathering• lead the criminal investigation (local authority children's social care have the lead for the section 47 enquires and assessment of the child's welfare) where joint enquiries take place

Flow chart 4: Action following a strategy discussion



Initiating section 47 enquiries

A section 47 enquiry is carried out by undertaking or continuing with an assessment in accordance with the guidance set out in this chapter and following the principles and parameters of a good assessment.

Local authority social workers should lead assessments under section 47 of the Children Act 1989. The police, health practitioners, teachers and school staff and other relevant practitioners should help the local authority in undertaking its enquiries.

Purpose:	A section 47 enquiry is initiated to decide whether and what type of action is required to safeguard and promote the welfare of a child who is suspected of or likely to be suffering significant harm.
-----------------	---

- | | |
|-------------------------------|---|
| Social workers should: | <ul style="list-style-type: none">• lead the assessment in accordance with this guidance• carry out enquiries in a way that minimises distress for the child and family• see the child who is the subject of concern to ascertain their wishes and feelings; assess their understanding of their situation; assess their relationships and circumstances more broadly• interview parents/carers and determine the wider social and environmental factors that might impact on them and their child• systematically gather information about the child's and family's history• analyse the findings of the assessment and evidence about what interventions are likely to be most effective with other relevant practitioners.• determine the child's needs and the level of risk of harm faced by the child to inform what help should be provided and act to provide that help• follow the guidance set out in 'Achieving Best Evidence in Criminal Proceedings: Guidance on interviewing victims and witnesses, and guidance on using special measures', where a decision has been made to undertake a joint interview of the child as part of any criminal investigation³³ |
|-------------------------------|---|

³³ Ministry of Justice [Achieving Best Evidence in Criminal Proceedings: Guidance on interviewing victims and witnesses, and guidance on using special measures](#) (2011).

Initiating section 47 enquiries

The police should:	<ul style="list-style-type: none">• help other organisations and agencies understand the reasons for concerns about the child’s safety and welfare• decide whether or not police investigations reveal grounds for instigating criminal proceedings• make available to other practitioners any evidence gathered to inform discussions about the child’s welfare• follow the guidance set out in ‘Achieving Best Evidence in Criminal Proceedings: Guidance’ on interviewing victims and witnesses, and guidance on using special measures, where a decision has been made to undertake a joint interview of the child as part of the criminal investigations
Health practitioners should:	<ul style="list-style-type: none">• provide any of a range of specialist assessments. For example, paediatric or forensic medical assessments, physiotherapists, occupational therapists, speech and language therapists and/or child psychologists may be involved in specific assessments relating to the child’s developmental progress. The lead health practitioner (probably a consultant paediatrician, or possibly the child’s GP) may need to request and co-ordinate these assessments• ensure appropriate treatment and follow up health concerns, such as administration of missing vaccines
All involved practitioners should:	<ul style="list-style-type: none">• contribute to the assessment as required, providing information about the child and family• consider whether a joint enquiry/investigation team may need to speak to a child victim without the knowledge of the parent/carers• seek advice and guidance as required and in line with local practice guidance

Outcome of section 47 enquiries

Local authority social workers are responsible for deciding what action to take and how to proceed following section 47 enquiries.

If local authority children's social care decides not to proceed with a child protection conference then other practitioners involved with the child and family have the right to request that local authority children's social care convene a conference if they have serious concerns that a child's welfare may not be adequately safeguarded. As a last resort, the safeguarding partners should have in place a quick and straightforward means of resolving differences of opinion.

Where concerns of significant harm are not substantiated:

Social workers should:	<ul style="list-style-type: none">discuss the case with the child, parents and other practitionersdetermine whether support from any services may be helpful and help secure itconsider whether the child's health and development should be re-assessed regularly against specific objectives and decide who has responsibility for doing this
All involved practitioners should:	<ul style="list-style-type: none">participate in further discussions as necessarycontribute to the development of any plan as appropriateprovide services as specified in the plan for the childreview the impact of services delivered as agreed in the planseek advice and guidance as required and in line with local practice guidance

Where concerns of significant harm are substantiated and the child is judged to be suffering or likely to suffer significant harm:

<p>Social workers should:</p>	<ul style="list-style-type: none"> • convene an initial child protection conference (see next section for details). The timing of this conference should depend on the urgency of the case and respond to the needs of the child and the nature and severity of the harm they may be facing. The initial child protection conference should take place within 15 working days of a strategy discussion, or the strategy discussion at which section 47 enquiries were initiated if more than one has been held • consider whether any practitioners with specialist knowledge should be invited to participate • ensure that the child and their parents understand the purpose of the conference and who will attend • help prepare the child if they are attending or making representations through a third party to the conference. Give information about advocacy agencies and explain that the family may bring an advocate, friend or supporter
<p>All involved practitioners should:</p>	<ul style="list-style-type: none"> • contribute to the information their agency provides ahead of the conference, setting out the nature of the organisation's or agency's involvement with the child and family • consider, in conjunction with the police and the appointed conference Chair, whether the report can and should be shared with the parents and if so when • attend the conference and take part in decision making when invited • seek advice and guidance as required and in line with local practice guidance

Initial child protection conferences

Following section 47 enquiries, an initial child protection conference brings together family members (and the child where appropriate), with the supporters, advocates and practitioners most involved with the child and family, to make decisions about the child's future safety, health and development. If concerns relate to an unborn child, consideration should be given as to whether to hold a child protection conference prior to the child's birth.

<p>Purpose:</p>	<p>To bring together and analyse, in an inter-agency setting, all relevant information and plan how best to safeguard and promote the welfare of the child. It is the responsibility of the conference to make recommendations on how organisations and agencies work together to safeguard the child in future. Conference tasks include:</p> <p>appointing a lead statutory body (either local authority children's social care or NSPCC) and a lead social worker, who should be a qualified, experienced social worker and an employee of the lead statutory body</p> <p>identifying membership of the core group of practitioners and family members who will develop and implement the child protection plan</p> <p>establishing timescales for meetings of the core group, production of a child protection plan and for child protection review meetings</p> <p>agreeing an outline child protection plan, with clear actions and timescales, including a clear sense of how much improvement is needed, by when, so that success can be judged clearly</p>
<p>The Conference Chair:</p>	<p>is accountable to the Director of Children's Services. Where possible the same person should chair subsequent child protection reviews</p> <p>should be a practitioner, independent of operational and/or line management responsibilities for the case</p> <p>should meet the child and parents in advance to ensure they understand the purpose and the process</p>
<p>Social workers should:</p>	<p>convene, attend and present information about the reason for the conference, their understanding of the child's needs, parental capacity and family and environmental context and evidence of how the child has been abused or neglected and its impact on their health and development</p>

Initial child protection conferences

	<p>analyse the information to enable informed decisions about what action is necessary to safeguard and promote the welfare of the child who is the subject of the conference</p> <p>share the conference information with the child and family beforehand (where appropriate)</p> <p>prepare a report for the conference on the child and family which sets out and analyses what is known about the child and family and the local authority's recommendation</p> <p>record conference decisions and recommendations and ensure action follows</p>
All involved practitioners should:	work together to safeguard the child from harm in the future, taking timely, effective action according to the plan agreed
Safeguarding partners should:	monitor the effectiveness of these arrangements

The child protection plan

Actions and responsibilities following the initial child protection conference

<p>Purpose:</p>	<p>The aim of the child protection plan is to:</p> <ul style="list-style-type: none"> ensure the child is safe from harm and prevent them from suffering further harm promote the child's health and development support the family and wider family members to safeguard and promote the welfare of their child, provided it is in the best interests of the child
<p>Local authority children's social care should:</p>	<ul style="list-style-type: none"> designate a social worker to be the lead practitioner as they carry statutory responsibility for the child's welfare consider the evidence and decide what legal action to take if any, where a child has suffered or is likely to suffer significant harm define the local protocol for timeliness of circulating plans after the child protection conference
<p>Social workers should:</p>	<ul style="list-style-type: none"> be the lead practitioner for inter-agency work with the child and family, co-ordinating the contribution of family members and practitioners into putting the child protection plan into effect develop the outline child protection plan into a more detailed interagency plan and circulate to relevant practitioners (and family where appropriate) ensure the child protection plan is aligned and integrated with any associated offender risk management plan undertake direct work with the child and family in accordance with the child protection plan, taking into account the child's wishes and feelings and the views of the parents in so far as they are consistent with the child's welfare complete the child's and family's in-depth assessment, securing contributions from core group members and others as necessary explain the plan to the child in a manner which is in accordance with their age and understanding and agree the plan with the child consider the need to inform the relevant Embassy if the child has links to a foreign country co-ordinate reviews of progress against the planned outcomes set out in the plan, updating as required. The first review should be held within three months

The child protection plan

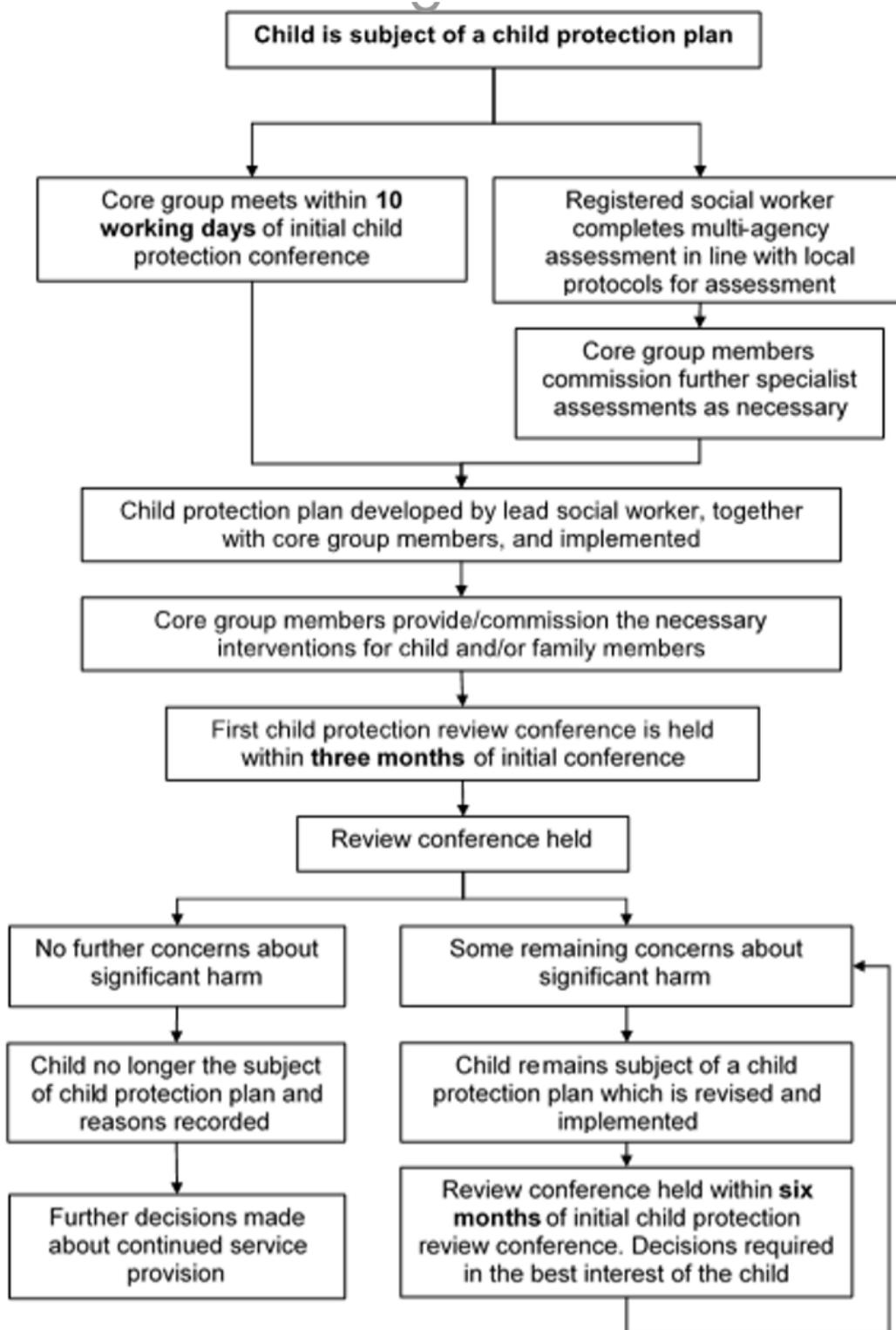
	<p>of the initial conference and further reviews at intervals of no more than six months for as long as the child remains subject of a child protection plan</p> <p>record decisions and actions agreed at core group meetings as well as the written views of those who were not able to attend, and follow up those actions to ensure they take place. The child protection plan should be updated as necessary</p> <p>lead core group activity</p>
The core group should:	<p>meet within 10 working days from the initial child protection conference if the child is the subject of a child protection plan</p> <p>further develop the outline child protection plan, based on assessment findings, and set out what needs to change, by how much, and by when in order for the child to be safe and have their needs met</p> <p>decide what steps need to be taken, and by whom, to complete the in-depth assessment to inform decisions about the child's safety and welfare</p> <p>implement the child protection plan and take joint responsibility for carrying out the agreed tasks, monitoring progress and outcomes, and refining the plan as needed</p>

Child protection review conference

The review conference procedures for preparation, decision-making and other procedures should be the same as those for an initial child protection conference.

Purpose:	<p>To review whether the child is continuing to suffer or is likely to suffer significant harm, and review developmental progress against child protection plan outcomes.</p> <p>To consider whether the child protection plan should continue or should be changed.</p>
Social workers should:	<ul style="list-style-type: none"> • attend and lead the organisation of the conference • determine when the review conference should be held within three months of the initial conference, and thereafter at maximum intervals of six months • provide information to enable informed decisions about what action is necessary to safeguard and promote the welfare of the child who is the subject of the child protection plan, and about the effectiveness and impact of action taken so far • share the conference information with the child and family beforehand, where appropriate • record conference outcomes • decide whether to initiate family court proceedings (all the children in the household should be considered, even if concerns are only expressed about one child) if the child is considered to be suffering significant harm
All involved practitioners should:	<ul style="list-style-type: none"> • attend, when invited, and provide details of their involvement with the child and family • produce reports for the child protection review. This information will provide an overview of work undertaken by family members and practitioners, and evaluate the impact on the child’s welfare against the planned outcomes set out in the child protection plan.

Flow chart 5: What happens after the child protection conference, including the review?



Discontinuing the Child Protection Plan

A child should no longer be the subject of a child protection plan if:

- it is judged that the child is no longer continuing to or is likely to suffer significant harm and therefore no longer requires safeguarding by means of a child protection plan
- the child and family have moved permanently to another local authority area. In such cases, the receiving local authority should convene a child protection conference within 15 working days of being notified of the move. Only after this event may the original local authority discontinue its child protection plan
- the child has reached 18 years of age (to end the child protection plan, the local authority should have a review around the child's birthday and this should be planned in advance), has died or has permanently left the United Kingdom

Social workers should:

- notify, as a minimum, all agency representatives who were invited to attend the initial child protection conference that led to the plan
- consider whether support services are still required and discuss with the child and family what might be needed, based on a re-assessment of the child's needs

Children returning home

Where the decision to return a child to the care of their family is planned, the local authority should undertake an assessment while the child is looked-after – as part of the care planning process (under regulation 39 of the Care Planning Regulations 2010). This assessment should consider what services and support the child (and their family) might need. The outcome of this assessment should be included in the child's care plan. The decision to cease to look after a child will, in most cases, require approval under regulation 39 of the Care Planning Regulations 2010.

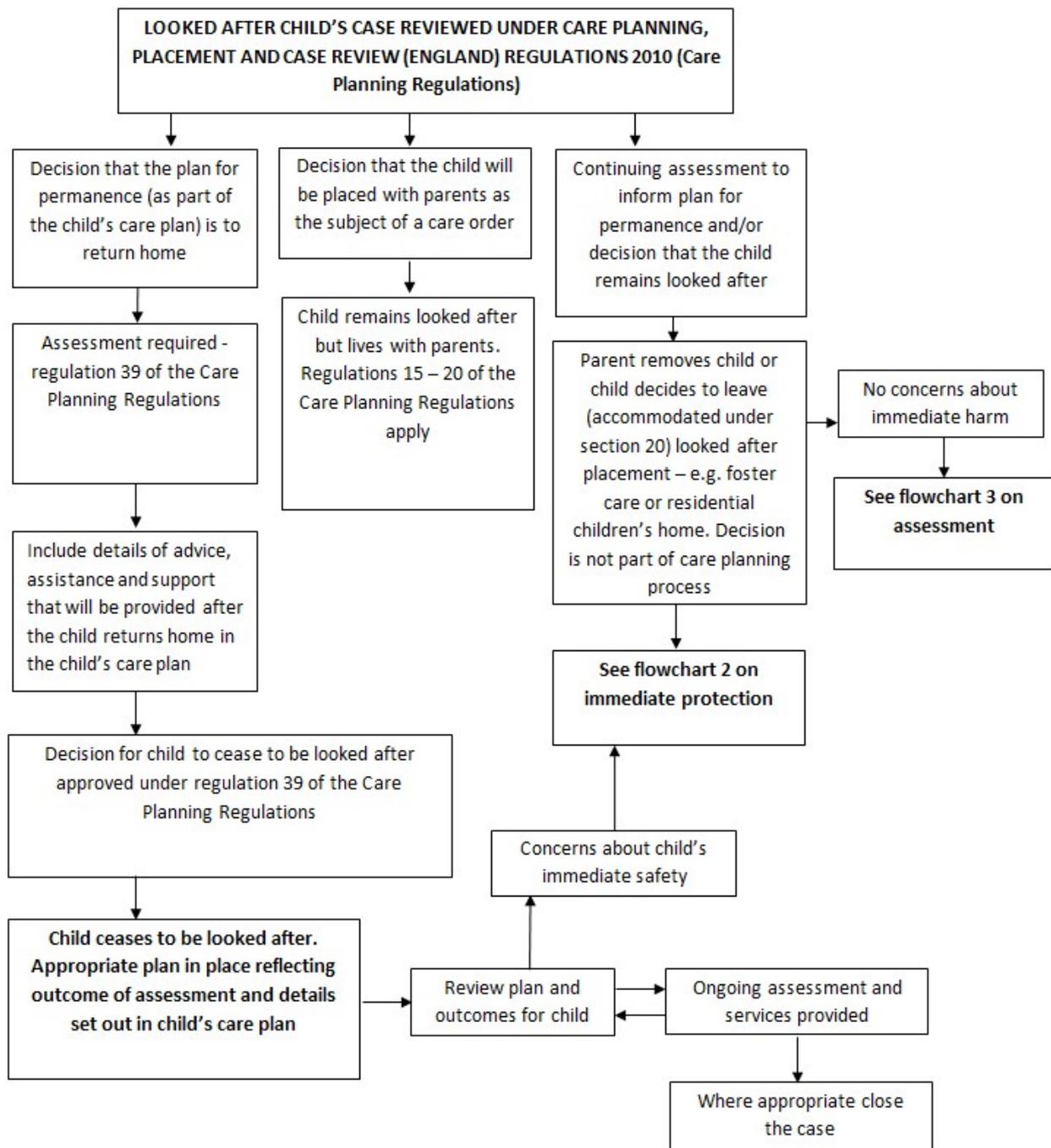
Where a child who is accommodated under section 20 returns home in an unplanned way, for example, the decision is not made as part of the care planning process but the parent removes the child or the child decides to leave, the local authority must consider whether there are any immediate concerns about the safety and wellbeing of the child. If there are concerns about a child's safety the local authority should take appropriate action, including that the local authority must make enquiries under section 47 of the Children Act 1989 if there is concern that the child is suffering or likely to suffer significant harm.

There should be a clear plan for all children who return home that reflects current and previous assessments, focuses on outcomes and includes details of services and support required. Action to be taken following reunification:

- practitioners should make the timeline and decision making process for providing ongoing services and support clear to the child and family
- when reviewing outcomes, children should, wherever possible, be seen alone. Practitioners have a duty to ascertain their wishes and feelings regarding the provision of services being delivered
- the impact of services and support should be monitored and recorded, and where a child is remanded to local authority or youth detention accommodation, consideration must be given to what on-going support and accommodation the child may need after their period of remand³⁴. This should be included in either their care plan or, if remanded to youth detention accommodation, detention placement plan.

³⁴ [The Children Act 1989 Guidance and Regulations Volume 2: Care, planning, placement and case review](#) paragraph 8.20.

Flow chart 6: Children returning home from care to their families



Chapter 2: Organisational responsibilities

1. The previous chapter set out how organisations and agencies should take a co-ordinated approach to ensure children are effectively safeguarded. A range of individual organisations and agencies working with children and families have specific statutory duties to promote the welfare of children and ensure they are protected from harm. These duties, as applied to individual organisations and agencies, are set out in this chapter.

Section 11 of the Children Act 2004

Places duties on a range of organisations, agencies and individuals to ensure their functions, and any services that they contract out to others, are discharged having regard to the need to safeguard and promote the welfare of children.

2. **Section 11** places a duty on:

- local authorities and district councils that provide children's and other types of services, including children's and adult social care services, public health, housing, sport, culture and leisure services, licensing authorities and youth services
- NHS organisations and agencies and the independent sector, including NHS England and clinical commissioning groups, NHS Trusts, NHS Foundation Trusts and General Practitioners
- the police, including police and crime commissioners and the chief officer of each police force in England and the Mayor's Office for Policing and Crime in London
- the British Transport Police
- the National Probation Service and Community Rehabilitation Companies³⁵
- Governors/Directors of Prisons and Young Offender Institutions (YOIs)
- Directors of Secure Training Centres (STCs)
- Principals of Secure Colleges
- Youth Offending Teams/Services (YOTs)

3. These organisations and agencies should have in place arrangements that reflect the importance of safeguarding and promoting the welfare of children, including:

- a clear line of accountability for the commissioning and/or provision of services designed to safeguard and promote the welfare of children

³⁵ The section 11 duty is conferred on the Community Rehabilitation Companies by virtue of contractual arrangements entered into with the Secretary of State.

- a senior board level lead with the required knowledge, skills and expertise or sufficiently qualified and experienced to take leadership responsibility for the organisation's/agency's safeguarding arrangements
- a culture of listening to children and taking account of their wishes and feelings, both in individual decisions and the development of services
- clear whistleblowing procedures, which reflect the principles in Sir Robert Francis' Freedom to Speak Up Review and are suitably referenced in staff training and codes of conduct, and a culture that enables issues about safeguarding and promoting the welfare of children to be addressed³⁶
- clear escalation policies for staff to follow when their child safeguarding concerns are not being addressed within their organisation or by other agencies
- arrangements which set out clearly the processes for sharing information, with other practitioners and with safeguarding partners
- a designated practitioner (or, for health commissioning and health provider organisations/agencies, designated and named practitioners) for child safeguarding. Their role is to support other practitioners in their organisations and agencies to recognise the needs of children, including protection from possible abuse or neglect. Designated practitioner roles should always be explicitly defined in job descriptions. Practitioners should be given sufficient time, funding, supervision and support to fulfil their child welfare and safeguarding responsibilities effectively
- safe recruitment practices and ongoing safe working practices for individuals whom the organisation or agency permit to work regularly with children, including policies on when to obtain a criminal record check
- appropriate supervision and support for staff, including undertaking safeguarding training
- creating a culture of safety, equality and protection within the services they provide

In addition:

- employers are responsible for ensuring that their staff are competent to carry out their responsibilities for safeguarding and promoting the welfare of children and creating an environment where staff feel able to raise concerns and feel supported in their safeguarding role

³⁶ [Sir Robert Francis' Freedom to speak up review](#).

- staff should be given a mandatory induction, which includes familiarisation with child protection responsibilities and the procedures to be followed if anyone has any concerns about a child's safety or welfare
- all practitioners should have regular reviews of their own practice to ensure they have knowledge, skills and expertise that improve over time

People in positions of trust

4. Organisations and agencies working with children and families should have clear policies for dealing with allegations against people who work with children. Such policies should make a clear distinction between an allegation, a concern about the quality of care or practice or a complaint. An allegation may relate to a person who works with children who has:

- behaved in a way that has harmed a child, or may have harmed a child
- possibly committed a criminal offence against or related to a child
- behaved towards a child or children in a way that indicates they may pose a risk of harm to children

5. County level and unitary local authorities should ensure that allegations against people who work with children are not dealt with in isolation. Any action necessary to address corresponding welfare concerns in relation to the child or children involved should be taken without delay and in a co-ordinated manner. Local authorities should, in addition, have designated a particular officer, or team of officers (either as part of local multi-agency arrangements or otherwise), to be involved in the management and oversight of allegations against people who work with children. Any such officer, or team of officers, should be sufficiently qualified and experienced to be able to fulfil this role effectively, for example, qualified social workers. Any new appointments to such a role, other than current or former designated officers moving between local authorities, should be qualified social workers. Arrangements should be put in place to ensure that any allegations about those who work with children are passed to the designated officer, or team of officers, without delay.

6. Local authorities should put in place arrangements to provide advice and guidance to employers and voluntary organisations and agencies on how to deal with allegations against people who work with children. Local authorities should also ensure that there are appropriate arrangements in place to liaise effectively with the police and other organisations and agencies to monitor the progress of cases and ensure that they are dealt with as quickly as possible, consistent with a thorough and fair process.

7. Employers, school governors, trustees and voluntary organisations should ensure that they have clear policies in place setting out the process, including timescales for investigation and what support and advice will be available to individuals against whom allegations have been made. Any allegation against people who work with children should be reported immediately to a senior manager within the organisation or agency. The designated officer, or team of officers, should also be informed within one working day of all allegations that come to an employer's attention or that are made directly to the police.

8. If an organisation or agency removes an individual (paid worker or unpaid volunteer) from work in regulated activity³⁷ with children (or would have, had the person not left first) because the person poses a risk of harm to children, the organisation or agency must make a referral to the Disclosure and Barring Service to consider whether to add the individual to the barred list.

9. This applies irrespective of whether a referral has been made to local authority children's social care and/or the designated officer or team of officers. It is an offence to fail to make a referral without good reason³⁸.

Individual organisational responsibilities

10. In addition to these section 11 duties, which apply to a number of named organisations and agencies, further safeguarding duties are also placed on individual organisations and agencies through other statutes. The key duties that fall on each individual organisation are set out below.

Schools, colleges and other educational providers

11. The following have duties in relation to safeguarding and promoting the welfare of children:

- governing bodies of maintained schools (including maintained nursery schools), further education colleges and sixth-form colleges³⁹

³⁷ [Regulated activity in relation to children: scope](#)

³⁸ Further guidance on referrals to the DBS is available at Appendix B

³⁹ Further education colleges and sixth-form colleges as established under the [Further Education and Higher Education Act 1992 and institutions designated as being within the further education sector. It relates to their responsibilities towards children who are receiving education or training at the college.](#)

- proprietors of academy schools, free schools, alternative provision academies and non-maintained special schools^{40,41}. In the case of academies and free school trusts, the proprietor will be the trust itself
- proprietors of independent schools
- management committees of pupil referral units⁴²

12. This guidance applies in its entirety to all schools.

13. Schools, colleges and other educational settings must also have regard to statutory guidance Keeping Children Safe in Education, which provides further guidance as to how they should fulfil their duties in respect of safeguarding and promoting the welfare of children in their care⁴³.

Early Years and Childcare

14. Early years providers have a duty under section 40 of the Childcare Act 2006 to comply with the welfare requirements of the early years foundation stage (EYFS)⁴⁴. Early years providers must ensure that:

- they are alert to any issues of concern in the child's life
- they have and implement a policy and procedures to safeguard children. This must include an explanation of the action to be taken when there are safeguarding concerns about a child and in the event of an allegation being made against a member of staff. The policy must also cover the use of mobile phones and cameras in the setting, that staff complete safeguarding training that enables them to understand their safeguarding policy and procedures, have up-to-date knowledge of safeguarding issues, and recognise signs of potential abuse and neglect
- they have a practitioner who is designated to take lead responsibility for safeguarding children within each early years setting and who must liaise with local statutory children's services as appropriate. This lead must also complete child protection training

⁴⁰ Under the Education (Independent School Standards) (England) Regulations 2014

⁴¹ Under [the Education \(Non-Maintained Special Schools\) \(England\) Regulations 2011](#)

⁴² Section 175, Education Act 2002 for management committees of pupil referral units, this is by virtue of regulation 3 and paragraph 19A of Schedule 1 to [the Education \(Pupil Referral Units\) \(Application of Enactments\) \(England\) Regulations 2007](#).

⁴³ [Keeping Children Safe in Education](#).

⁴⁴ [Section 3 – safeguarding and welfare requirements in the Statutory Framework for the Early Years Foundation Stage](#).

Health

15. Clinical commissioning groups are one of the three statutory safeguarding partners as set out in chapter 3. NHS organisations and agencies are subject to the section 11 duties set out in this chapter. Health practitioners are in a strong position to identify welfare needs or safeguarding concerns regarding individual children and, where appropriate, provide support. This includes understanding risk factors, communicating and sharing information effectively with children and families, liaising with other organisations and agencies, assessing needs and capacity, responding to those needs and contributing to multi-agency assessments and reviews.

16. A wide range of health practitioners have a critical role to play in safeguarding and promoting the welfare of children including: GPs, primary care practitioners, paediatricians, nurses, health visitors, midwives, school nurses, allied health practitioners, those working in maternity, child and adolescent mental health, youth custody establishments, adult mental health, sexual, alcohol and drug services for both adults and children, unscheduled and emergency care settings, highly specialised services and secondary and tertiary care.

17. All staff working in healthcare settings – including those who predominantly treat adults – should receive training to ensure they attain the competences appropriate to their role and follow the relevant professional guidance^{45,46,47}.

18. Within the NHS⁴⁸:

- **NHS England** is responsible for ensuring that the health commissioning system as a whole is working effectively to safeguard and promote the welfare of children. It is also accountable for the services it directly commissions, including primary care, and healthcare services in the under-18 secure estate (for police custody settings see below in the policing section). NHS England also leads and defines improvement in safeguarding practice and outcomes and should also ensure that there are effective mechanisms for safeguarding partners and Health and wellbeing boards to raise concerns about the engagement and leadership of the local NHS. Each NHSE region should have a safeguarding lead to ensure regional collaboration and assurance through convening safeguarding forums

⁴⁵ [Safeguarding Children and Young People: roles and competences for health care staff](#), RCPCH (2014).

⁴⁶ [Looked-after children: Knowledge, skills and competences of health care staff](#), RCN and RCPCH, (2015).

⁴⁷ For example, [Protecting children and young people: the responsibilities of all doctors](#), GMC (2018) and [Safeguarding Children and Young People: The RCGP/NSPCC Safeguarding Children Toolkit for General Practice](#), RCGP (2014).

⁴⁸ Further guidance on accountabilities for safeguarding children in the NHS is available in [Safeguarding Vulnerable People in the Reformed NHS: Accountability and Assurance Framework](#) (2015).

- Clinical commissioning groups are one of the statutory safeguarding partners and the major commissioners of local health services. They are responsible for the provision of effective clinical, professional and strategic leadership to child safeguarding, including the quality assurance of safeguarding through their contractual arrangements with all provider organisations and agencies, including from independent providers

Designated health professionals

19. Clinical commissioning groups should employ, or have in place, a contractual agreement to secure the expertise of designated practitioners; such as dedicated designated doctors and nurses for safeguarding children and dedicated designated doctors and nurses for looked-after children (and designated doctor or paediatrician for unexpected deaths in childhood).

20. In some areas, there will be more than one clinical commissioning group per local authority, and they may consider 'lead' or 'hosting' arrangements for their designated health professionals, or a clinical network arrangement with the number of Designated Doctors and Nurses for child safeguarding equating to the size of the child population⁴⁹. Designated doctors and nurses, as senior professionals, clinical experts and strategic leaders, are a vital source of safeguarding advice and expertise for all relevant organisations and agencies but particularly the clinical commissioning group, NHS England, and the local authority, and for advice and support to other health practitioners across the health economy. The NHS commissioners and providers should ensure that designated professionals are given sufficient time to be fully engaged, involved and included in the new safeguarding arrangements.

21. All providers of NHS funded health services including NHS Trusts and NHS Foundation Trusts should identify a dedicated named doctor and a named nurse (and a named midwife if the organisation or agency provides maternity services) for safeguarding children. In the case of ambulance trusts and independent providers, this should be a named practitioner. Named practitioners have a key role in promoting good professional practice within their organisation and agency, providing advice and expertise for fellow practitioners, and ensuring safeguarding training is in place. They should work closely with their organisation's/agency's safeguarding lead on the executive board, designated health professionals for the health economy and other statutory safeguarding partners⁵⁰.

⁴⁹ Safeguarding children and young people: roles and competencies for health care staff

⁵⁰ Model job descriptions for designated and named professional roles can be found in the intercollegiate document Safeguarding children and young people: roles and competences for health care staff and Safeguarding Children and Young People: The RCGP/NSPCC Safeguarding Children Toolkit for General Practice, RCGP (2014)

22. Clinical commissioning groups should employ a named GP to advise and support GP safeguarding practice leads. GPs should have a lead and deputy lead for safeguarding, who should work closely with the named GP based in the clinical commissioning group⁵¹.

23. Other public, voluntary and independent sector organisations, agencies and social enterprises providing NHS services to children and families should ensure that they follow this guidance.

Public Health England

24. Public Health England (PHE) is an executive agency of the Department of Health and Social Care which has operational autonomy to advise and support government, local authorities and the NHS in a professionally independent manner. PHE's mission is "to protect and improve the nation's health and to address inequalities", and was established in 2013 following the Health and Social Care Act 2012. PHE's Chief Nurse provides advice and expertise in their capacity as the government's professional advisor (Public Health Nursing), which in the context of children's health includes health visitors and school nurses.

Police

25. The police are one of the three statutory safeguarding partners as set out in chapter 3 and are subject to the section 11 duties set out in this chapter. Under section 1(8)(h) of the Police Reform and Social Responsibility Act 2011, the Police and Crime Commissioner (PCC) must hold the Chief Constable to account for the exercise of the latter's duties in relation to safeguarding children under sections 10 and 11 of the Children Act 2004.

26. All police officers, and other police employees such as Police Community Support Officers, are well placed to identify early when a child's welfare is at risk and when a child may need protection from harm. Children have the right to the full protection offered by criminal law. In addition to identifying when a child may be a victim of a crime, police officers should be aware of the effect of other incidents which might pose safeguarding risks to children and where officers should pay particular attention. For example, an officer attending a domestic abuse incident should be aware of the effect of such behaviour on any children in the household. Children who are encountered as offenders, or alleged offenders, are entitled to the same safeguards and protection as any other child and due regard should be given to their safety and welfare at all times. For example, children who

⁵¹ Intercollegiate framework: Safeguarding children and young people: roles and competencies for healthcare staff

are apprehended in possession of Class A drugs may be victims of exploitation through county lines drug dealing.

27. The police will hold important information about children who may be suffering, or likely to suffer, significant harm, as well as those who cause such harm. They should always share this information with other organisations and agencies where this is necessary to protect children. Similarly, they can expect other organisations and agencies to share information to enable the police to carry out their duties. All police forces should have officers trained in child abuse investigation.

28. The police have a power to remove a child to suitable accommodation under section 46 of the Children Act 1989, if they have reasonable cause to believe that the child would otherwise be likely to suffer significant harm. Statutory powers to enter premises can be used with this section 46 power, and in circumstances to ensure the child's immediate protection. Police powers can help in emergency situations, but should be used only when necessary and, wherever possible, the decision to remove a child from a parent or carer should be made by a court.

29. Restrictions and safeguards exist in relation to the circumstances and periods for which children may be taken to or held in police stations⁵². PCCs are responsible for health commissioning in police custody settings and should always ensure that this meets the needs of individual children.

Adult social care services

30. Local authorities provide services to adults who are themselves responsible for children who may be in need. These services are subject to the section 11 duties set out in this chapter. When staff are providing services to adults they should ask whether there are children in the family and consider whether the children need help or protection from harm. Children may be at greater risk of harm or be in need of additional help in families where the adults have mental health problems, misuse drugs or alcohol, are in a violent relationship, have complex needs or have learning difficulties.

⁵² Potential powers of entry include those under:

- Police and Criminal Evidence Act 1984 (PACE) [section 17\(1\)\(b\)](#), a constable may enter and search any premises for the purpose of arresting a person for an indictable offence
- PACE [section 17\(1\)\(e\)](#), a constable may also enter and search premises for the purpose of saving life or limb or preventing serious damage to property – in the exercise of [police protection](#) powers if entry to premises is refused, this section may give adequate powers;
- common law, where a constable has the power to enter premises to prevent or deal with a breach of the peace (which is preserved under PACE [section 17\(6\)](#));
- Children Act 1989 [section 48](#), a warrant may be obtained to search for children who may be in need of emergency protection.

31. Adults with parental responsibilities for disabled children have a right to a separate parent carer's needs assessment under section 17ZD of the Children Act 1989. Adults who do not have parental responsibility, but are caring for a disabled child, are entitled to an assessment on their ability to provide, or to continue to provide, care for that disabled child under the Carers (Recognition and Services) Act 1995. That assessment must also consider whether the carer works or wishes to work, or whether they wish to engage in any education, training or recreation activities.

32. Adult social care services should liaise with children's social care services to ensure that there is a joined-up approach when carrying out such assessments.

Housing services

33. Housing and homelessness services in local authorities and others such as environmental health organisations are subject to the section 11 duties set out in this chapter. Practitioners working in these services may become aware of conditions that could have or are having an adverse impact on children. Under Part 1 of the Housing Act 2004, authorities must take account of the impact of health and safety hazards in housing on vulnerable occupants, including children, when deciding on the action to be taken by landlords to improve conditions. Housing authorities also have an important role to play in safeguarding vulnerable young people, including young people who are pregnant, leaving care or a secure establishment.

British Transport Police

34. The British Transport Police (BTP) is subject to the section 11 duties set out in this chapter. In its role as the national police for the railways, the BTP can play an important role in safeguarding and promoting the welfare of children, especially in identifying and supporting children who have run away, are truanting from school or who are being exploited by criminal gangs to move drugs and money.

35. The BTP should carry out its duties in accordance with its legislative powers. This includes removing a child to a suitable place using their police protection powers under the Children Act 1989, and the protection of children who are truanting from school using powers under the Crime and Disorder Act 1998. This involves, for example, the appointment of a designated independent officer in the instance of a child taken into police protection.

Prison Service

36. The Prison Service is subject to the section 11 duties set out in this chapter. It also has a responsibility to identify prisoners who are potential or confirmed 'persons posing a risk to children' (PPRC) and through assessment establish whether the PPRC presents a continuing risk to children whilst in prison custody^{53,54}. Where an individual has been identified as a PPRC, the relevant prison establishment:

- should inform the local authority children's social care services of the offender's reception to prison, subsequent transfers, release on temporary licence and of release date and of the release address of the offender
- should notify the relevant probation service provider of PPRC status. The police should also be notified of the release date and address^{55,56}
- may prevent or restrict a prisoner's contact with children. Decisions on the level of contact, if any, should be based on a multi-agency risk assessment. The assessment should draw on relevant risk information held by police, the probation service provider and the prison service. The relevant local authority children's social care should contribute to the multi-agency risk assessment by providing a report on the child's best interests. The best interests of the child will be paramount in the decision-making process⁵⁷

37. A prison is also able to monitor an individual's communication (including letters and telephone calls) to protect children where it is proportionate and necessary to the risk presented.

38. Governors/Directors of women's prisons which have Mother and Baby Units (MBUs) should ensure that:

- there is at all times a member of staff allocated to the MBU, who as a minimum, is trained in first aid, whilst within the prison there is always a member of staff on duty who is trained in paediatric first aid (including child/adult resuscitation) who can be called to the MBU if required
- there is a contingency plan/policy in place for child protection, first aid including paediatric first aid and resuscitation, which should include advice for managing

⁵³ This applies not just to adult prisons but also to all types of establishments within the secure estate for children, with the same process applying to children who pose a risk to other children.

⁵⁴ [HMP Public Protection Manual](#)

⁵⁵ Should the PPRC have been released under probation supervision, the prison no longer has responsibility for them and it falls to the NPS/CRC to address and manage the risk in the community.

⁵⁶ The management of an individual who presents a risk of harm to children will often be through a multidisciplinary Interdepartmental Risk Management Team (IRMT).

⁵⁷ Ministry of Justice [Chapter 2, Section 2 of HM Prison Service Public Protection Manual](#).

such events, and which provides mothers with detailed guidance as to what to do in an emergency

- each baby has a child care plan setting out how the best interests of the child will be maintained and promoted during the child's residence in the unit

This also applies to MBUs which form part of the secure estate for children.

Probation Service

39. Probation services are provided by the National Probation Service (NPS) and 21 Community Rehabilitation Companies (CRCs). The NPS and CRCs are subject to the section 11 duties set out in this chapter⁵⁸. They are primarily responsible for working with adult offenders both in the community and in the transition from custody to community to reduce reoffending and improve rehabilitation. During the course of their duties, probation staff come into contact with offenders who:

- have offended against a child
- pose a risk of harm to children even though they have not been convicted of an offence against a child
- are parents and/or carers of children
- have regular contact with a child for whom they do not have caring responsibility

They are, therefore, well placed to identify offenders who pose a risk of harm to children as well as children who may be at heightened risk of involvement in, or exposure to, criminal or anti-social behaviour, and of other poor outcomes due to the behaviour and/or home circumstances of their parent/carer(s).

40. They should ask an offender at the earliest opportunity whether they live with, have caring responsibilities for, are in regular contact with, or are seeking contact with children. Where this applies, a check should be made with the local authority children's services at the earliest opportunity on whether the child/children is/are known to them and, if they are, the nature of their involvement.

41. Where an adult offender is assessed as presenting a risk of serious harm to children, the offender manager should develop a risk management plan and supervision plan that contains a specific objective to manage and reduce the risk of harm to children. The risk management plan should be shared with other organisations and agencies involved in the risk management.

⁵⁸ The section 11 duty is conferred on the Community Rehabilitation Companies by virtue of contractual arrangements entered into with the Secretary of State.

42. In preparing a sentence plan, offender managers should consider how planned interventions might bear on parental responsibilities and whether the planned interventions could contribute to improved outcomes for children known to be in an existing relationship with the offender.

Children's homes

43. The registered person of a children's home must have regard to the Guide to the Children's Homes Regulations, including the quality standards (April 2015), in interpreting and meeting the Regulations. The Guide covers the quality standards for children's homes, which set out the aspirational and positive outcomes that we expect homes to achieve, including the standard for the protection of children. The registered person is responsible for ensuring that staff continually and actively assess the risks to each child and the arrangements in place to protect them. Where there are safeguarding concerns for a child, their placement plan, agreed between the home and their placing authority, must include details of the steps the home will take to manage any assessed risks on a day to day basis.

44. In addition to the requirements of this standard, the registered person has specific responsibilities under regulation 34 to prepare and implement policies setting out: arrangements for the safeguarding of children from abuse or neglect; clear procedures for referring child protection concerns to the placing authority or local authority where the home is situated if appropriate; and specific procedures to prevent children going missing and take action if they do.

45. Each home should work with their local safeguarding partners to agree how they will work together, and with the placing authority, to make sure that the needs of the individual children are met.

The secure estate for children

46. Governors, managers, directors and principals of the following secure establishments are subject to the section 11 duties set out in this chapter:

- a secure training centre
- a young offender institution
- a secure college/school

47. Each centre holding those aged under 18 should have in place an annually-reviewed safeguarding children policy. The policy is designed to promote and safeguard the welfare of children and should cover all relevant operational areas as well as key supporting processes, which would include issues such as child protection, risk of harm,

restraint, separation, staff recruitment and information sharing. A manager should be appointed and will be responsible for implementation of this policy⁵⁹.

48. Each centre should work with their local safeguarding partners to agree how they will work together, and with the relevant YOT and placing authority (the Youth Custody Service), to make sure that the needs of individual children are met.

Youth Offending Teams

49. YOTs are subject to the section 11 duties set out in this chapter. YOTs are multi-agency teams responsible for the supervision of children subject to pre-court interventions and statutory court disposals⁶⁰. They are therefore well placed to identify children known to relevant organisations and agencies as being most at risk of offending and the contexts in which they may be vulnerable to abuse, and to undertake work to prevent them offending or protect them from harm. YOTs should have a lead officer responsible for ensuring safeguarding is embedded in their practice.

50. Under section 38 of the Crime and Disorder Act 1998, local authorities must, within the delivery of youth justice services, ensure the ‘provision of persons to act as appropriate adults to safeguard the interests of children detained or questioned by police officers’.

UK Visas and Immigration, Immigration Enforcement and the Border Force

51. Section 55 of the Borders, Citizenship and Immigration Act 2009 places upon the Secretary of State a duty to make arrangements to take account of the need to safeguard and promote the welfare of children in discharging functions relating to immigration, asylum, nationality and customs. These functions are discharged on behalf of the Secretary of State by UK Visas and Immigration, Immigration Enforcement and the Border Force, which are part of the Home Office. The statutory guidance Arrangements to Safeguard and Promote Children’s Welfare and other guidance relevant to the discharge of specific immigration functions set out these arrangements⁶¹.

⁵⁹ Detailed guidance on the safeguarding children policy, the roles of the safeguarding children manager and the safeguarding children committee, and the role of the establishment in relation to the LSCB can be found in [Prison Service Instruction \(PSI\) 08/2012 ‘Care and Management of Young People’](#).

⁶⁰ The statutory membership of YOTs is set out in [section 39 \(5\) of the Crime and Disorder Act 1998](#).

⁶¹ [Arrangements to Safeguard and Promote Children’s Welfare in the United Kingdom Border Agency](#). (original title “Every Child Matters” statutory guidance to the UK Border Agency under section 55 of the Borders, Citizenship and Immigration Act 2009).

Children and Family Court Advisory and Support Service

52. The responsibility of the Children and Family Court Advisory and Support Service (Cafcass), as set out in the Children Act 1989, is to safeguard and promote the welfare of individual children who are the subject of family court proceedings. This is through the provision of independent social work advice to the court.

53. A Cafcass officer has a statutory right in public law cases to access local authority records relating to the child concerned and any application under the Children Act 1989. That power also extends to other records that relate to the child and the wider functions of the local authority, or records held by an authorised organisation that relate to that child.

54. Where a Cafcass officer has been appointed by the court as a child's guardian and the matter before the court relates to specified proceedings, they should be invited to all formal planning meetings convened by the local authority in respect of the child. This includes statutory reviews of children who are accommodated or looked-after, child protection conferences and relevant adoption panel meetings.

Armed Services

55. Local authorities have the statutory responsibility for safeguarding and promoting the welfare of the children of service families in the UK^{62,63}. In discharging these responsibilities:

- local authorities should ensure that the Ministry of Defence, soldiers, sailors, airmen, and Families Association Forces Help, the British Forces Social Work Service or the Naval Personal and Family Service is made aware of any service child who is the subject of a child protection plan and whose family is about to move overseas
- each local authority with a United States (US) base in its area should establish liaison arrangements with the base commander and relevant staff. The requirements of English child welfare legislation should be explained clearly to the US authorities, so that the local authority can fulfil its statutory duties

⁶² When service families or civilians working with the armed forces are based overseas the responsibility for safeguarding and promoting the welfare of their children is vested in the Ministry of Defence. The Ministry of Defence contact is through the Directorate of Children and Young People: Tel 01980 618710 or email DCYP-DCYP-MAILBOX@mod.uk

⁶³ The Army welfare contact is through the Army Welfare Service Intake and Assessment Team: Tel. 01904 882053 or email: RC-AWS-IAT-0Mailbox@mod.uk ; The Naval Service welfare contact is through the RN RM Welfare (RNRMW) Portal. Tel: 02392 728777 or email NAVYNPS-PEOPLESTRNRMPORTAL@mod.uk; The RAF welfare contact is through the Personal Support and Social Work Service RAF (SSAFA): Tel: 03000 111 723 or email psswsRAF@ssafa.org.uk

Multi-Agency Public Protection Arrangements

56. Many of the agencies subject to the section 11 duty are members of the Multi-Agency Public Protection Arrangements (MAPPA), including the police, prison and probation services. MAPPA should work together with duty to co-operate (DTC)⁶⁴ agencies to manage the risks posed by violent and sexual offenders living in the community in order to protect the public and should work closely with the safeguarding partners over services to commission locally.

Voluntary, charity, social enterprise, faith-based organisations and private sectors

57. Voluntary, charity, social enterprise (VCSE) and private sector organisations and agencies play an important role in safeguarding children through the services they deliver. Some of these will work with particular communities, with different races and faith communities and delivering in health, adult social care, housing, prisons and probation services. They may as part of their work provide a wide range of activities for children and have an important role in safeguarding children and supporting families and communities.

58. Like other organisations and agencies who work with children, they should have appropriate arrangements in place to safeguard and protect children from harm. Many of these organisations and agencies as well as many schools, children's centres, early years and childcare organisations, will be subject to charity law and regulated either by the Charity Commission or other "principal" regulators. Charity trustees are responsible for ensuring that those benefiting from, or working with, their charity, are not harmed in any way through contact with it. The Charity Commission for England and Wales provides guidance on charity compliance which should be followed. Further information on the Charity Commission's role in safeguarding can be found on: [the Charity Commission's page on Gov.uk](#).

59. Some of these organisations and agencies are large national charities whilst others will have a much smaller local reach. Some will be delivering statutory services and may be run by volunteers, such as library services. This important group of organisations includes youth services not delivered by local authorities or district councils.

60. All practitioners working in these organisations and agencies who are working with children and their families are subject to the same safeguarding responsibilities, whether paid or a volunteer.

⁶⁴ The DTC agencies are listed in section 325(6) of the CJA 2003. They are required to co-operate as far as they can do so, consistent with the exercise of their other statutory functions.

61. Every VCSE, faith-based organisation and private sector organisation or agency should have policies in place to safeguard and protect children from harm. These should be followed and systems should be in place to ensure compliance in this. Individual practitioners, whether paid or volunteer, should be aware of their responsibilities for safeguarding and protecting children from harm, how they should respond to child protection concerns and how to make a referral to local authority children's social care or the police if necessary.

62. Every VCSE, faith-based organisation and private sector organisation or agency should have in place the arrangements described in this chapter. They should be aware of how they need to work with the safeguarding partners in a local area. Charities (within the meaning of section 1 Charities Act 2011), religious organisations (regulation 34 and schedule 3 to School Admissions) and any person involved in the provision, supervision or oversight of sport or leisure are included within the relevant agency regulations. This means if the safeguarding partners name them as a relevant partner they must cooperate. Other VCSE, faith-based and private sector organisations not on the list of relevant agencies can also be asked to cooperate as part of the local arrangements and should do so.

Sports Clubs / Organisations

63. There are many sports clubs and organisations including voluntary and private sector providers that deliver a wide range of sporting activities to children. Some of these will be community amateur sports clubs, some will be charities. All should have the arrangements described in this chapter in place and should collaborate to work effectively with the safeguarding partners as required by any local safeguarding arrangements. Paid and volunteer staff need to be aware of their responsibilities for safeguarding and promoting the welfare of children, how they should respond to child protection concerns and how to make a referral to local authority children's social care or the police if necessary.

64. All National Governing Bodies of Sport, that receive funding from either Sport England⁶⁵ or UK Sport⁶⁶, must aim to meet the Standards for Safeguarding and Protecting Children in Sport⁶⁷.

⁶⁵ [Sport England](#)

⁶⁶ [UK Sport](#)

⁶⁷ [Standards for Safeguarding and Protecting Children in Sport.](#)

Chapter 3: Multi-agency safeguarding arrangements

1. Local organisations and agencies that work with children and families play a significant role when it comes to safeguarding children.
2. To achieve the best possible outcomes, children and families should receive targeted services that meet their needs in a co-ordinated way. Fragmented provision of services creates inefficiencies and risks disengagement by children and their families from services such as GPs, education and wider voluntary and community specialist support.
3. There is a shared responsibility between organisations and agencies to safeguard and promote the welfare of all children in a local area.
4. As set out in chapter 2, many local organisations and agencies have a duty under section 11 of the Children Act 2004 to ensure that they consider the need to safeguard and promote the welfare of children when carrying out their functions.
5. The responsibility for this join-up locally rests with the three safeguarding partners who have a shared and equal duty to make arrangements to work together to safeguard and promote the welfare of all children in a local area.

Safeguarding partners

Safeguarding partners ⁶⁸

A *safeguarding partner* in relation to a local authority area in England is defined under the Children Act 2004 (as amended by the Children and Social Work Act, 2017) as:

- (a) the local authority
- (b) a clinical commissioning group for an area any part of which falls within the local authority area
- (c) the chief officer of police for an area any part of which falls within the local authority area

6. The three safeguarding partners should agree on ways to co-ordinate their safeguarding services; act as a strategic leadership group in supporting and engaging others; and implement local and national learning including from serious child safeguarding incidents (see chapter 4).

⁶⁸ Children Act 2004, Section 16E

7. To fulfil this role, the three safeguarding partners must set out how they will work together and with any relevant agencies. Relevant agencies are those organisations and agencies whose involvement the safeguarding partners consider may be required to safeguard and promote the welfare of children with regard to local need.

8. The purpose of these local arrangements is to support and enable local organisations and agencies to work together in a system where:

- children are safeguarded and their welfare promoted
- partner organisations and agencies collaborate, share and co-own the vision for how to achieve improved outcomes for vulnerable children
- organisations and agencies challenge appropriately and hold one another to account effectively
- there is early identification and analysis of new safeguarding issues and emerging threats
- learning is promoted and embedded in a way that local services for children and families can become more reflective and implement changes to practice
- information is shared effectively to facilitate more accurate and timely decision making for children and families

9. In order to work together effectively, the safeguarding partners with other local organisations and agencies should develop processes that:

- facilitate and drive action beyond usual institutional and agency constraints and boundaries
- ensure the effective protection of children is founded on practitioners developing lasting and trusting relationships with children and their families

10. To be effective, these arrangements should link to other strategic partnership work happening locally to support children and families. This will include other public boards including Health and wellbeing boards, Adult Safeguarding Boards, Channel Panels, Improvement Boards, Community Safety Partnerships, the Local Family Justice Board and MAPPAs.

Leadership

11. Strong leadership is critical for the new arrangements to be effective in bringing together the various organisations and agencies. It is important therefore that the lead representative from each of the three safeguarding partners plays an active role. The lead representatives for safeguarding partners are: the local authority chief executive, the accountable officer of a clinical commissioning group, and a chief officer of police.

12. All three safeguarding partners have equal and joint responsibility for local safeguarding arrangements. In situations that require a clear, single point of leadership, all three safeguarding partners should decide who would take the lead on issues that arise.

13. Should the lead representatives delegate their functions they remain accountable for any actions or decisions taken on behalf of their agency. If delegated, it is the responsibility of the lead representative to identify and nominate a senior officer in their agency to have responsibility and authority for ensuring full participation with these arrangements.

14. The representatives, or those they delegate authority to, should be able to:

- speak with authority for the safeguarding partner they represent
- take decisions on behalf of their organisation or agency and commit them on policy, resourcing and practice matters
- hold their own organisation or agency to account on how effectively they participate and implement the local arrangements

Geographical area

15. The geographical footprint for the new arrangements is based on local authority areas. A single local authority area cannot be covered by two separate safeguarding partnerships. Every local authority, clinical commissioning group and police force must be covered by a local safeguarding arrangement. Local arrangements can cover two or more local authorities. Where more than one local authority joins together, the local authorities can agree to delegate their safeguarding partner duties to a single authority⁶⁹. Each local authority must continue to fulfil its statutory and legislative duties to safeguard and promote the welfare of children. The same applies for clinical commissioning groups and chief officers of police (in respect of their safeguarding partner duties only).

16. The administrative geography of safeguarding partners can be changed over time. Where changes are proposed, these should be agreed by the three safeguarding partners, communicated clearly to relevant agencies and practitioners, and reflected in the next yearly report (see paragraph 42).

⁶⁹ Children Act 2004, Section 16J

Relevant agencies

17. As set out below, relevant agencies are those organisations and agencies whose involvement the safeguarding partners consider is required to safeguard and promote the welfare of local children. Strong, effective multi-agency arrangements are ones that are responsive to local circumstances and engage the right people. For local arrangements to be effective, they should engage organisations and agencies that can work in a collaborative way to provide targeted support to children and families as appropriate. This approach requires flexibility to enable joint identification of, and response to, existing and emerging needs, and to agree priorities to improve outcomes for children.

18. The safeguarding partners must set out in their published arrangements which organisations and agencies they will be working with to safeguard and promote the welfare of children, and this will be expected to change over time if the local arrangements are to work effectively for children and families. A list of relevant agencies is set out in regulations⁷⁰.

19. When selected by the safeguarding partners to be part of the local safeguarding arrangements, relevant agencies must act in accordance with the arrangements⁷¹. Safeguarding partners should make sure the relevant agencies are aware of the expectations placed on them by the new arrangements. They should consult relevant agencies in developing the safeguarding arrangements to make sure the expectations take account of an agency's structure and statutory obligations.

20. Where a relevant agency has a national remit, such as the British Transport Police and Cafcass, safeguarding partners should be clear on how these agencies should collaborate and take account of that agency's individual responsibilities and potential contributions towards a number of local safeguarding arrangements. The involvement of health providers and commissioners will be different in each local area and local safeguarding partners should consider how they will secure the clinical expertise of designated health professionals for safeguarding children within their arrangements.

21. The published arrangements should set out clearly any contributions agreed with relevant agencies, including funding, accommodation, services and any resources connected with the arrangements.

22. In setting out how they will work with relevant agencies, the safeguarding partners should be clear how they will assure themselves that relevant agencies have appropriate, robust safeguarding policies and procedures in place and how information will be shared amongst all relevant agencies and the safeguarding partners.

⁷⁰ [The Child Safeguarding Practice Review and Relevant Agency \(England\) Regulations 2018](#)

⁷¹ Children Act 2004, Section 16G

23. Many agencies and organisations play a crucial role in safeguarding children. Safeguarding partners may include any local or national organisation or agency in their arrangements, regardless of whether they are named in relevant agency regulations. Organisations and agencies who are not named in the relevant agency regulations, whilst not under a statutory duty, should nevertheless cooperate and collaborate with the safeguarding partners particularly as they may have duties under section 10 and/or section 11 of the Children Act 2004.

24. Safeguarding partners should communicate regularly with their relevant agencies and others they expect to work with them. It is for the safeguarding partners to determine how regularly their list of relevant agencies will be reviewed. The local arrangements should be shared with all partners and relevant agencies, and information should be given about how to escalate concerns and how any disputes will be resolved. This should give details of the independent scrutiny and whistleblowing procedures.

Schools, colleges and other educational providers

25. Schools, colleges and other educational providers have a pivotal role to play in safeguarding children and promoting their welfare. Their co-operation and buy-in to the new arrangements will be vital for success. All schools, colleges and other educational providers have duties in relation to safeguarding children and promoting their welfare. The statutory guidance 'Keeping Children Safe in Education' should be read alongside this guidance.

26. The safeguarding partners should make arrangements to allow all schools (including multi academy trusts), colleges and other educational providers, in the local area to be fully engaged, involved and included in the new safeguarding arrangements. It is expected that local safeguarding partners will name schools, colleges and other educational providers as relevant agencies and will reach their own conclusions on how best locally to achieve the active engagement of individual institutions in a meaningful way.

27. Once designated as a relevant agency, schools and colleges, and other educational providers, in the same way as other relevant agencies, are under a statutory duty to co-operate with the published arrangements.

Information requests

28. Organisations and agencies within a strong multi-agency system should have confidence that information is shared effectively, amongst and between them, to improve outcomes for children and their families. Safeguarding partners may require any person or organisation or agency to provide them, any relevant agency for the area, a reviewer or

another person or organisation or agency, with specified information. This must be information which enables and assists the safeguarding partners to perform their functions to safeguard and promote the welfare of children in their area, including as related to local and national child safeguarding practice reviews.

29. The person or organisation to whom a request is made must comply with such a request and if they do not do so, the safeguarding partners may take legal action against them.

30. As public authorities, safeguarding partners should be aware of their own responsibilities under the relevant information law and have regard to guidance provided by the Information Commissioner's Office when issuing and responding to requests for information.

Independent scrutiny

31. The role of independent scrutiny is to provide assurance in judging the effectiveness of multi-agency arrangements to safeguard and promote the welfare of all children in a local area, including arrangements to identify and review serious child safeguarding cases⁷². This independent scrutiny will be part of a wider system which includes the independent inspectorates' single assessment of the individual safeguarding partners and the Joint Targeted Area Inspections.

32. Whilst the decision on how best to implement a robust system of independent scrutiny is to be made locally, safeguarding partners should ensure that the scrutiny is objective, acts as a constructive critical friend and promotes reflection to drive continuous improvement.

33. The independent scrutineer should consider how effectively the arrangements are working for children and families as well as for practitioners, and how well the safeguarding partners are providing strong leadership and agree with the safeguarding partners how this will be reported.

34. The published arrangements should set out the plans for independent scrutiny; how the arrangements will be reviewed; and how any recommendations will be taken forward. This might include, for example, the process and timescales for ongoing review of the arrangements.

35. Safeguarding partners should also agree arrangements for independent scrutiny of the report they must publish at least once a year (see 'Reporting', below).

⁷² See chapter 4

Funding

36. Working in partnership means organisations and agencies should collaborate on how they will fund their arrangements. The three safeguarding partners and relevant agencies for the local authority area should make payments towards expenditure incurred in conjunction with local multi-agency arrangements for safeguarding and promoting welfare of children.

37. The safeguarding partners should agree the level of funding secured from each partner, which should be equitable and proportionate, and any contributions from each relevant agency, to support the local arrangements. The funding should be transparent to children and families in the area, and sufficient to cover all elements of the arrangements, including the cost of local child safeguarding practice reviews.

Publication of arrangements

38. Once agreed, local safeguarding arrangements must be published and must include:

- arrangements for the safeguarding partners to work together to identify and respond to the needs of children in the area
- arrangements for commissioning and publishing local child safeguarding practice reviews (see chapter 4)
- arrangements for independent scrutiny of the effectiveness of the arrangements

39. They should also include:

- who the three local safeguarding partners are, especially if the arrangements cover more than one local authority area
- geographical boundaries (especially if the arrangements operate across more than one local authority area)
- the relevant agencies the safeguarding partners will work with; why these organisations and agencies have been chosen; and how they will collaborate and work together to improve outcomes for children and families
- how all early years settings, schools (including independent schools, academies and free schools) and other educational establishments will be included in the safeguarding arrangements
- how any youth custody and residential homes for children will be included in the safeguarding arrangements

- how the safeguarding partners will use data and intelligence to assess the effectiveness of the help being provided to children and families, including early help
- how inter-agency training will be commissioned, delivered and monitored for impact and how they will undertake any multiagency and interagency audits
- how the arrangements will be funded
- the process for undertaking local child safeguarding practice reviews, setting out the arrangements for embedding learning across organisations and agencies,
- how the arrangements will include the voice of children and families
- how the threshold document⁷³ setting out the local criteria for action aligns with the arrangements

Dispute resolution

40. Safeguarding partners and relevant agencies must act in accordance with the arrangements for their area, and will be expected to work together to resolve any disputes locally. Public bodies that fail to comply with their obligations under law are held to account through a variety of regulatory and inspection activity. In extremis, any non-compliance will be referred to the Secretary of State.

Reporting

41. In order to bring transparency for children, families and all practitioners about the activity undertaken, the safeguarding partners must publish a report at least once in every 12-month period. The report must set out what they have done as a result of the arrangements, including on child safeguarding practice reviews, and how effective these arrangements have been in practice.

42. In addition, the report should also include:

- evidence of the impact of the work of the safeguarding partners and relevant agencies, including training, on outcomes for children and families from early help to looked-after children and care leavers
- an analysis of any areas where there has been little or no evidence of progress on agreed priorities

⁷³ see Chapter 1: Assessing need and providing help

- a record of decisions and actions taken by the partners in the report's period (or planned to be taken) to implement the recommendations of any local and national child safeguarding practice reviews, including any resulting improvements
- ways in which the partners have sought and utilised feedback from children and families to inform their work and influence service provision

43. Safeguarding partners should make sure the report is widely available, and the published safeguarding arrangements should set out where the reports will be published.

44. A copy of all published reports should be sent to the Child Safeguarding Practice Review Panel⁷⁴ and the What Works Centre for Children's Social Care within seven days of being published.

45. Where there is a secure establishment in a local area, safeguarding partners should include a review of the use of restraint within that establishment in their report, and the findings of the review should be reported to the Youth Justice Board.

46. The three safeguarding partners should report any updates to the published arrangements in their yearly report and the proposed timescale for implementation.

⁷⁴ Children Act 2004, Section 16F (3)(c)

Chapter 4: Improving child protection and safeguarding practice

Overview

1. Child protection in England is a complex multi-agency system with many different organisations and individuals playing their part. Reflecting on how well that system is working is critical as we constantly seek to improve our collective public service response to children and their families.

2. Sometimes a child suffers a serious injury or death as a result of child abuse or neglect. Understanding not only what happened but also why things happened as they did can help to improve our response in the future. Understanding the impact that the actions of different organisations and agencies had on the child's life, and on the lives of his or her family, and whether or not different approaches or actions may have resulted in a different outcome, is essential to improve our collective knowledge. It is in this way that we can make good judgments about what might need to change at a local or national level.

Purpose of child safeguarding practice reviews

3. The purpose of reviews of serious child safeguarding cases, at both local and national level, is to identify improvements to be made to safeguard and promote the welfare of children. Learning is relevant locally, but it has a wider importance for all practitioners working with children and families and for the government and policy-makers. Understanding whether there are systemic issues, and whether and how policy and practice need to change, is critical to the system being dynamic and self-improving.

4. Reviews should seek to prevent or reduce the risk of recurrence of similar incidents. They are not conducted to hold individuals, organisations or agencies to account, as there are other processes for that purpose, including through employment law and disciplinary procedures, professional regulation and, in exceptional cases, criminal proceedings. These processes may be carried out alongside reviews or at a later stage. Employers should consider whether any disciplinary action should be taken against practitioners whose conduct and/or practice falls below acceptable standards and should refer to their regulatory body as appropriate.

Responsibilities for reviews

5. The responsibility for how the system learns the lessons from serious child safeguarding incidents lies at a national level with the Child Safeguarding Practice Review Panel (the Panel) and at local level with the safeguarding partners.
6. The Panel is responsible for identifying and overseeing the review of serious child safeguarding cases which, in its view, raise issues that are complex or of national importance. The Panel should also maintain oversight of the system of national and local reviews and how effectively it is operating.
7. Locally, safeguarding partners must make arrangements to identify and review serious child safeguarding cases which, in their view, raise issues of importance in relation to their area. They must commission and oversee the review of those cases, where they consider it appropriate for a review to be undertaken.
8. The Panel and the safeguarding partners have a shared aim in identifying improvements to practice and protecting children from harm and should maintain an open dialogue on an ongoing basis. This will enable them to share concerns, highlight commonly-recurring areas that may need further investigation (whether leading to a local or national review), and share learning, including from success, that could lead to improvements elsewhere.
9. Safeguarding partners should have regard to any guidance which the Panel publishes. Guidance will include the timescales for rapid reviews (see paragraph 20) and for the Panel response.
10. Serious child safeguarding cases are those in which:
 - abuse or neglect of a child is known or suspected **and**
 - the child has died or been seriously harmed
11. Serious harm includes (but is not limited to) serious **and/or** long-term impairment of a child's mental health or intellectual, emotional, social or behavioural development. It should also cover impairment of physical health⁷⁵. This is not an exhaustive list. When making decisions, judgment should be exercised in cases where impairment is likely to be long-term, even if this is not immediately certain. Even if a child recovers, including from a one-off incident, serious harm may still have occurred.

⁷⁵ Child perpetrators may also be the subject of a review, if the definition of 'serious child safeguarding case' is met.

Duty on local authorities to notify incidents to the Child Safeguarding Practice Review Panel

16C(1) of the Children Act 2004 (as amended by the Children and Social Work Act 2017) states:

Where a local authority in England knows or suspects that a child has been abused or neglected, the local authority must notify the Child Safeguarding Practice Review Panel if –

- (a) the child dies or is seriously harmed in the local authority's area, or
- (b) while normally resident in the local authority's area, the child dies or is seriously harmed outside England.

12. The local authority must notify any event that meets the above criteria to the Panel⁷⁶. They should do so within five working days of becoming aware that the incident has occurred. The local authority should also report the event to the safeguarding partners in their area (and in other areas if appropriate⁷⁷) within five working days.

13. The local authority must **also** notify the Secretary of State and Ofsted where a looked after child has died, whether or not abuse or neglect is known or suspected.

14. The duty to notify events to the Panel rests with the local authority. Others who have functions relating to children⁷⁸ should inform the safeguarding partners of any incident which they think should be considered for a child safeguarding practice review. The link to the Child Safeguarding Online Notification form for local authorities to notify incidents to the Panel is available from [Report a serious child safeguarding incident page on Gov.uk](#)

Decisions on local and national reviews

15. Safeguarding partners must make arrangements to:

- identify serious child safeguarding cases which raise issues of importance in relation to the area **and**

⁷⁶ Online notifications to the Panel will be shared with Ofsted (to inform its inspection and regulatory activity) and with DfE to enable it to carry out its functions.

⁷⁷ If, for example, the event relates to a looked after child who has been placed out of area.

⁷⁸ This means any person or organisation with statutory or official duties or responsibilities relating to children.

- commission and oversee the review of those cases, where they consider it appropriate for a review to be undertaken

16. When a serious incident becomes known to the safeguarding partners⁷⁹, they must consider whether the case meets the criteria for a local review.

17. Meeting the criteria does not mean that safeguarding partners must automatically carry out a local child safeguarding practice review. It is for them to determine whether a review is appropriate, taking into account that the overall purpose of a review is to identify improvements to practice. Issues might appear to be the same in some child safeguarding cases but reasons for actions and behaviours may be different and so there may be different learning to be gained from similar cases. Decisions on whether to undertake reviews should be made transparently and the rationale communicated appropriately, including to families.

18. Safeguarding partners must consider the criteria and guidance below when determining whether to carry out a local child safeguarding practice review.

The criteria which the local safeguarding partners must take into account include whether the case⁸⁰:

- highlights or may highlight improvements needed to safeguard and promote the welfare of children, including where those improvements have been previously identified
- highlights or may highlight recurrent themes in the safeguarding and promotion of the welfare of children
- highlights or may highlight concerns regarding two or more organisations or agencies working together effectively to safeguard and promote the welfare of children
- is one which the Child Safeguarding Practice Review Panel have considered and concluded a local review may be more appropriate

⁷⁹ Safeguarding partners should also take account of information from other sources if applicable.

⁸⁰ [The Child Safeguarding Practice Review and Relevant Agency \(England\) Regulations 2018](#).

Safeguarding partners should also have regard to the following circumstances:

- where the safeguarding partners have cause for concern about the actions of a single agency
- where there has been no agency involvement and this gives the safeguarding partners cause for concern
- where more than one local authority, police area or clinical commissioning group is involved, including in cases where families have moved around
- where the case may raise issues relating to safeguarding or promoting the welfare of children in institutional settings⁸¹

19. Some cases may not meet the definition of a 'serious child safeguarding case', but nevertheless raise issues of importance to the local area. That might, for example, include where there has been good practice, poor practice or where there have been 'near miss' events. Safeguarding partners may choose to undertake a local child safeguarding practice review in these or other circumstances.

The rapid review

20. The safeguarding partners should promptly undertake a rapid review of the case, in line with any guidance published by the Panel. The aim of this rapid review is to enable safeguarding partners to:

- gather the facts about the case, as far as they can be readily established at the time
- discuss whether there is any immediate action needed to ensure children's safety and share any learning appropriately
- consider the potential for identifying improvements to safeguard and promote the welfare of children
- decide what steps they should take next, including whether or not to undertake a child safeguarding practice review

21. As soon as the rapid review is complete, the safeguarding partners should send a copy to the Panel⁸². They should also share with the Panel their decision about whether a

⁸¹ Includes children's homes (including secure children's homes) and other settings with residential provision for children; custodial settings where a child is held, including police custody, young offender institutions and secure training centres; and all settings where detention of a child takes place, including under the Mental Health Act 1983 or the Mental Capacity Act 2005.

⁸² The Panel may share this with DfE if requested, to enable DfE to carry out its functions.

local child safeguarding practice review is appropriate, or whether they think the case may raise issues which are complex or of national importance such that a national review may be appropriate. They may also do this if, during the course of a local child safeguarding practice review, new information comes to light which suggests that a national review may be appropriate. As soon as they have determined that a local review will be carried out, they should inform the Panel, Ofsted and DfE, including the name of any reviewer they have commissioned.

Guidance for the national Child Safeguarding Practice Review Panel

22. On receipt of the information from the rapid review, the Panel must decide whether it is appropriate to commission a national review of a case or cases. They must consider the criteria and guidance below.

The criteria which the Panel must take into account include whether the case⁸³:

- highlights or may highlight improvements needed to safeguard and promote the welfare of children, including where those improvements have been previously identified
- raises or may raise issues requiring legislative change or changes to guidance issued under or further to any enactment
- highlights or may highlight recurrent themes in the safeguarding and promotion of the welfare of children

The Panel should also have regard to the following circumstances:

- significant harm or death to a child educated otherwise than at school
- where a child is seriously harmed or dies while in the care of a local authority, or while on (or recently removed from) a child protection plan
- cases which involve a range of types of abuse⁸⁴
- where the case may raise issues relating to safeguarding or promoting the welfare of children in institutional settings⁸⁵

⁸³ [The Child Safeguarding Practice Review and Relevant Agency \(England\) Regulations 2018](#)

⁸⁴ For example, trafficking for the purposes of child sexual exploitation.

⁸⁵ Includes children's homes (including secure children's homes) and other settings with residential provision for children; custodial settings where a child is held, including police custody, young offender institutions and secure training centres; and all settings where detention of a child takes place, including under the Mental Health Act 1983 or the Mental Capacity Act 2005.

23. As well as considering notifications from local authorities and information from rapid reviews and local child safeguarding practice reviews, the Panel should take into account a range of other evidence, including inspection reports and other reports and research. The Panel may also take into account any other criteria they consider appropriate to identify whether a serious child safeguarding case raises issues which are complex or of national importance.

24. In many cases there will need to be dialogue between the safeguarding partners and the Panel to support the decision-making process. The safeguarding partners must share further information with the Panel as requested.

25. The Panel should inform the relevant safeguarding partners promptly following receipt of the rapid review, if they consider that:

- a national review is appropriate, setting out the rationale for their decision and next steps
- further information is required to support the Panel's decision-making (including whether the safeguarding partners have taken a decision as to whether to commission a local review)

26. The Panel should take decisions on whether to undertake national reviews and communicate their rationale appropriately, including to families. The Panel should notify the Secretary of State when a decision is made to carry out a national review.

27. If the Panel decides to undertake a national review they should discuss with the safeguarding partners the potential scope and methodology of the review and how they will engage with them and those involved in the case.

28. There will be instances where a local review has been carried out which could then form part of a thematic review that the Panel undertakes at a later date. There may also be instances when a local review has not been carried out but where the Panel considers that the case could be helpful to a national review at some stage in the future. In such circumstances, the Panel should engage with safeguarding partners to agree the conduct of the review.

29. Alongside any national or local reviews, there could be a criminal investigation, a coroner's investigation and/or professional body disciplinary procedures. The Panel and the safeguarding partners should have clear processes for how they will work with other investigations, including Domestic Homicide Reviews, multi-agency public protection arrangements reviews or Safeguarding Adults Reviews, and work collaboratively with those responsible for carrying out those reviews. This is to reduce burdens on and anxiety for the children and families concerned and to minimise duplication of effort and uncertainty.

Commissioning a reviewer or reviewers for a local child safeguarding practice review

30. The safeguarding partners are responsible for commissioning and supervising reviewers for local reviews⁸⁶.

31. In all cases they should consider whether the reviewer has the following:

- professional knowledge, understanding and practice relevant to local child safeguarding practice reviews, including the ability to engage both with practitioners and children and families
- knowledge and understanding of research relevant to children's safeguarding issues
- ability to recognise the complex circumstances in which practitioners work together to safeguard children
- ability to understand practice from the viewpoint of the individuals, organisations or agencies involved at the time rather than using hindsight
- ability to communicate findings effectively
- whether the reviewer has any real or perceived conflict of interest

Local child safeguarding practice reviews

32. The safeguarding partners should agree with the reviewer(s) the method by which the review should be conducted, taking into account this guidance and the principles of the systems methodology recommended by the Munro review⁸⁷. The methodology should provide a way of looking at and analysing frontline practice as well as organisational structures and learning. The methodology should be able to reach recommendations that will improve outcomes for children. All reviews should reflect the child's perspective and the family context.

33. The review should be proportionate to the circumstances of the case, focus on potential learning, and establish and explain the reasons why the events occurred as they did.

34. As part of their duty to ensure that the review is of satisfactory quality, the safeguarding partners should seek to ensure that:

⁸⁶ Safeguarding partners may also consider appointing reviewers from the Child Safeguarding Practice Review Panel's pool of reviewers where available.

⁸⁷ [The Munro Review of Child Protection: Final Report: A Child Centred System](#) (May 2011).

- practitioners are fully involved in reviews and invited to contribute their perspectives without fear of being blamed for actions they took in good faith
- families, including surviving children, are invited to contribute to reviews. This is important for ensuring that the child is at the centre of the process⁸⁸. They should understand how they are going to be involved and their expectations should be managed appropriately and sensitively

35. The safeguarding partners must supervise the review to ensure that the reviewer is making satisfactory progress and that the review is of satisfactory quality. The safeguarding partners may request information from the reviewer during the review to enable them to assess progress and quality; any such requests must be made in writing. The President of the Family Division's guidance covering the role of the judiciary in SCRs⁸⁹ should also be noted in the context of child safeguarding practice reviews.

Expectations for the final report

36. Safeguarding partners must ensure that the final report includes:

- a summary of any recommended improvements to be made by persons in the area to safeguard and promote the welfare of children
- an analysis of any systemic or underlying reasons why actions were taken or not in respect of matters covered by the report

37. Any recommendations should be clear on what is required of relevant agencies and others collectively and individually, and by when, and focussed on improving outcomes for children.

38. Reviews are about promoting and sharing information about improvements, both within the area and potentially beyond, so safeguarding partners must publish the report, unless they consider it inappropriate to do so. In such a circumstance, they must publish any information about the improvements that should be made following the review that they consider it appropriate to publish. The name of the reviewer(s) should be included. Published reports or information must be publicly available for at least one year.

39. When compiling and preparing to publish the report, the safeguarding partners should consider carefully how best to manage the impact of the publication on children, family members, practitioners and others closely affected by the case. The safeguarding

⁸⁸ [Morris, K., Brandon, M., and Tudor, P., \(2013\) 'Rights, Responsibilities and Pragmatic Practice: Family participation in Case Reviews'](#).

⁸⁹ [President of the Family Division's Guidance covering the role of the judiciary in serious case reviews.](#)

partners should ensure that reports are written in such a way so that what is published avoids harming the welfare of any children or vulnerable adults involved in the case.

40. Safeguarding partners must send a copy of the full report to the Panel and to the Secretary of State no later than seven working days⁹⁰ before the date of publication. Where the safeguarding partners decide only to publish information relating to the improvements to be made following the review, they must also provide a copy of that information to the Panel and the Secretary of State within the same timescale. They should also provide the report, or information about improvements, to Ofsted within the same timescale.

41. Depending on the nature and complexity of the case, the report should be completed and published as soon as possible and no later than six months from the date of the decision to initiate a review. Where other proceedings may have an impact on or delay publication, for example an ongoing criminal investigation, inquest or future prosecution, the safeguarding partners should inform the Panel and the Secretary of State of the reasons for the delay. Safeguarding partners should also set out for the Panel and the Secretary of State the justification for any decision not to publish either the full report or information relating to improvements. Safeguarding partners should have regard to any comments that the Panel or the Secretary of State may make in respect of publication.

42. Every effort should also be made, both before the review and while it is in progress, to (i) capture points from the case about improvements needed, and (ii) take corrective action and disseminate learning.

Actions in response to local and national reviews

43. The safeguarding partners should take account of the findings from their own local reviews and from all national reviews, with a view to considering how identified improvements should be implemented locally, including the way in which organisations and agencies work together to safeguard and promote the welfare of children. The safeguarding partners should highlight findings from reviews with relevant parties locally and should regularly audit progress on the implementation of recommended improvements⁹¹. Improvement should be sustained through regular monitoring and follow up of actions so that the findings from these reviews make a real impact on improving outcomes for children.

⁹⁰ 'Working day' means any day which is not a Saturday, Sunday or Bank Holiday.

⁹¹ See also paragraph 41 in chapter 3 (safeguarding partners' report).

Guidance for the Child Safeguarding Practice Review Panel – reviewers

44. The Panel must set up a pool of potential reviewers who can undertake national reviews, a list of whom must be publicly available. If they consider that there are no potential reviewers in the pool with availability or suitable experience to undertake the review, they may select a person who is not in the pool. When selecting a reviewer, the Panel should consider whether they have any conflict of interest which could restrict their ability, or perceived ability, to identify improvements impartially.

45. For national child safeguarding practice reviews, the Panel should follow the same guidance on procedure and supervision as for local child safeguarding practice reviews (paragraphs 32-35).

The Panel – expectations for the final report

46. The Panel must ensure that the final report includes:

- a summary of any improvements being recommended to the safeguarding partners and/or others to safeguard and promote the welfare of children
- an analysis of any systemic or underlying reasons why actions were taken or not taken in respect of matters covered by the report

47. The Panel must publish the report, unless they consider it inappropriate to do so. In such a circumstance they must publish any information about the improvements that should be made following the review that they consider it appropriate to publish. The name of the reviewer(s) should be included.

48. The Panel should work with safeguarding partners to identify and manage the impact of the publication on children, family members, practitioners and others closely affected by the case.

49. The Panel must ensure that reports or information published are publicly available for at least three years. The Panel must send a copy of the full report to the Secretary of State no later than seven working days before the date of publication. Where the Panel decides only to publish information relating to the improvements to be made following the review, they must also provide a copy of that information to the Secretary of State within the same timescale. The Panel should also send a copy of the report or improvements to the relevant safeguarding partners, Ofsted, the Care Quality Commission and Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services.

50. Reports should be completed and published within six months of the date of the decision to initiate a review. Where other proceedings may have an impact on or delay

publication, for example an ongoing criminal investigation, inquest or future prosecution, the Panel should advise the Secretary of State of the reasons for the delay. The Panel should also set out for the Secretary of State the explanation for any decision not to publish either the full report or information relating to improvements. During the review, the Panel should share any points that arise about improvements needed with the safeguarding partners in any local authority areas covered by the review and others as applicable.

51. The Panel should send copies of published reports of national and local child safeguarding practice reviews, or published information relating to improvements that should be made following those reviews, to the What Works Centre for Children's Social Care and relevant inspectorates, bodies or individuals as they see fit. Where a local review results in findings which are of national importance, or in recommendations for national government, the Panel should consider the potential of those recommendations to improve systems to safeguard and promote the welfare of children and how best to disseminate and embed such learning.

Chapter 5: Child death reviews

1. The death of a child is a devastating loss that profoundly affects all those involved. The process of systematically reviewing the deaths of children is grounded in respect for the rights of children and their families⁹², with the intention of learning what happened and why, and preventing future child deaths.

2. The majority of child deaths in England arise from medical causes. Enquiries should keep an appropriate balance between forensic and medical requirements and supporting the family at a difficult time. This chapter provides guidance to child death review partners in light of their statutory responsibilities.

3. Child death review partners are local authorities and any clinical commissioning groups for the local area as set out in the Children Act 2004 (the Act), as amended by the Children and Social Work Act 2017⁹³. The statutory responsibilities for child death review partners are set out in the table below, and the boundaries for child death review partners should be decided locally as described in paragraph 9 of this chapter.

4. In the immediate aftermath of a child's death, a copy of *When a Child Dies – a guide for families and carers*⁹⁴ should be offered to all bereaved families or carers in order to support them through the child death review process. In addition to supporting families and carers, staff involved in the care of the child should also be considered and offered appropriate support.

⁹² [United Nations Convention on the Rights of the Child](#)

⁹³ Sections 16Q

⁹⁴ [When a Child Dies – a guide for families and carers](#)

Statutory Requirements⁹⁵

When a child dies, in any circumstances, it is important for parents and families to understand what has happened and whether there are any lessons to be learned.

The responsibility for ensuring child death reviews are carried out is held by 'child death review partners,' who, in relation to a local authority area in England, are defined as the local authority for that area and any clinical commissioning groups operating in the local authority area.

Child death review partners must make arrangements to review all deaths of children normally resident in the local area⁹⁶ and, if they consider it appropriate, for any non-resident child who has died in their area.

Child death review partners for two or more local authority areas may combine and agree that their areas be treated as a single area for the purpose of undertaking child death reviews.

Child death review partners must make arrangements for the analysis of information from all deaths reviewed.

The purpose of a review and/or analysis is to identify any matters relating to the death, or deaths, that are relevant to the welfare of children in the area or to public health and safety, and to consider whether action should be taken in relation to any matters identified. If child death review partners find action should be taken by a person or organisation, they must inform them. In addition, child death review partners:

- must, at such times as they consider appropriate, prepare and publish reports on:
 - what they have done as a result of the child death review arrangements in their area, and
 - how effective the arrangements have been in practice;
- may request information from a person or organisation for the purposes of enabling or assisting the review and/or analysis process - the person or organisation must comply with the request, and if they do not, the child death review partners may take legal action to seek enforcement: and
- may make payments directly towards expenditure incurred in connection with arrangements made for child death reviews or analysis of information about deaths reviewed, or by contributing to a fund out of which payments may be made; and may provide staff, goods, services, accommodation or other resources to any person for purposes connected with the child death review or analysis process.

⁹⁵ The guidance in this chapter is issued under section 16Q of the Children Act 2004. Further guidance on child death review procedures will be issued by the government. While the contents of this chapter will be duplicated within that document, child death review partners should also have regard to that guidance to assist in their understanding of the steps taken by others prior to the child death reviews and analysis they carry out.

⁹⁶ For the purposes of child death reviews, a local area is the area within the remit of a local authority (referred to in the Act as a "local authority area").

Responsibilities of Child Death Review Partners

5. The child death review process covers children: a child is defined in the Act as a person under 18 years of age⁹⁷, regardless of the cause of death⁹⁸.
6. In making arrangements to review child deaths, child death review partners should establish a structure and process to review all deaths of children normally resident in their area and, if appropriate and agreed between child death review partners, the deaths of children not normally resident in their area but who have died there. Child death review partners may, if they consider it appropriate, model their child death review structures and processes on the current Child Death Overview Panel (CDOP) framework⁹⁹.
7. The child death review partners should consider the core representation of any panel or structure they set up to conduct reviews and this would ideally include: public health; the designated¹⁰⁰ doctor for child deaths for the local area; social services; police; the designated doctor or nurse for safeguarding; primary care (GP or health visitor); nursing and/or midwifery; lay representation; and other professionals that child death review partners consider should be involved. It is for child death review partners to determine what representation they have in any structure reviewing child deaths.
8. Child death review partners should agree locally how the child death review process will be funded in their area.
9. The geographical and population 'footprint' of child death review partners should be locally agreed, but must extend to at least one local authority area. This footprint should take into account networks of NHS care, and agency and organisational boundaries in order to reflect the integrated care and social networks of the local area. These may overlap with more than one local authority area or clinical commissioning group. They should cover a child population such that they typically review at least 60 child deaths per year. Child death review partners should come together to develop clear plans outlining the administrative and logistical processes for these new review arrangements.
10. Child death review partners should ensure that a designated doctor for child deaths is appointed to any multi-agency panel (or structure in place to review deaths). The designated doctor for child deaths should be a senior paediatrician who can take a lead role in the review process. Child death review partners should ensure a process is in

⁹⁷ Section 65 of the Children Act 2004.

⁹⁸ This will include the death of any new-born baby (of any gestation) who shows signs of life following birth, or where the birth was unattended, but does not include those (of any gestation) who are stillborn where there was medical attendance, or planned terminations of pregnancy carried out within the law.

⁹⁹ The CDOP frameworks were established and are currently used by Local Safeguarding Children Boards to review the deaths of children in their areas.

¹⁰⁰ Within that part of the health system that supports child safeguarding and protection services, the word "designated" means a dedicated professional with specific roles and responsibilities that are centred on the provision of clinical expertise and strategic advice.

place whereby the designated doctor for child deaths is notified of each child death and is sent relevant information.

11. Child death review partners may request a person or organisation to provide information to enable or assist the reviewing and/or analysing of a child's death. The person or organisation to whom a request is made must comply with such a request and if they do not do so, the child death review partners may instigate legal action to enforce.

12. Child death review partners for the local authority area where a child who has died was normally resident are responsible for ensuring the death is reviewed. However, they may also choose to review the death of a child in their local area even if that child is not normally resident there. Child death review partners may wish to consider this for the deaths of looked-after children in their area who were not normally resident there. The review process should seek to involve child death review partners for another local authority area who had an interest in the child or any other person or agencies, as appropriate.

13. Child death review partners should publicise information on the arrangements for child death reviews in their area. This should include who the accountable officials are (the local authority chief executive and the accountable officer of the clinical commissioning group), which local authority and clinical commissioning group partners are involved, what geographical area is covered and who the designated doctor for child deaths is.

Responsibilities of other organisations and agencies

14. All local organisations or individual practitioners that have had involvement in the case should co-operate, as appropriate, in the child death review process carried out by child death review partners. All local organisations or individual practitioners should also have regard to any guidance on child death reviews issued by the government.

Specific responsibilities of relevant bodies in relation to child deaths	
Registrars of Births and Deaths (Section 31 of the Children and Young Persons Act 2008)	Requirement on registrars of births and deaths to supply child death review partners with the particulars of the death entered in the register in relation to any person who was or may have been under the age of 18 at the time of death. A similar requirement exists where the registrar corrects an entry in the register. The registrar must also notify child death review partners if they issue a Certificate of No Liability to

	<p>Register (where a death is not required by law to be registered in England or Wales) where it appears that the deceased was or may have been under the age of 18 at the time of death.</p> <p>The information must be provided to the appropriate child death review partners (which cover the sub-district in which the register is kept) no later than seven days from either the date the death was registered, the date the correction was made or the date the certificate was issued¹⁰¹.</p>
<p>Coroners and Justice Act 2009</p> <p>Coroners (Investigations) Regulations 2013</p>	<p>Duty to investigate and hold an inquest. Powers to request a post-mortem and for evidence to be given or produced.</p> <p>Coroner's duty to notify the child death review partners¹⁰² for the area in which the child died or where the child's body was found within three working days of deciding to investigate a death or commission a post-mortem.</p> <p>Coroner's duty to share information with the relevant child death review partners¹⁰³.</p>

¹⁰¹ Amendments have been made to the Children and Young Persons Act. It should be noted that while these amendments came into force on 29th June 2018, they will not have effect in a local authority area until the date that area implements its new safeguarding partnership arrangements.

¹⁰² Amendments will be made to the Coroners (Investigations) Regulations 2013 to require the Coroner to notify the relevant safeguarding partners and child death review partners instead of LSCBs. Until such time as these amendments are made, where a local area has implemented its new safeguarding partnership arrangements, Coroners are asked to also notify relevant child death review partners.

¹⁰³ Amendments will be made to the (Investigations) Regulations 2013 to require the Coroner to share information with the relevant safeguarding partners and child death review partners instead of LSCBs. Until such time as these amendments are made, where a local area has implemented its new safeguarding partnership arrangements, Coroners are asked to also share information with the relevant child death review partners.

Responding to the death of a child: the child death review process

Flow Chart 7: Process to follow when a child dies

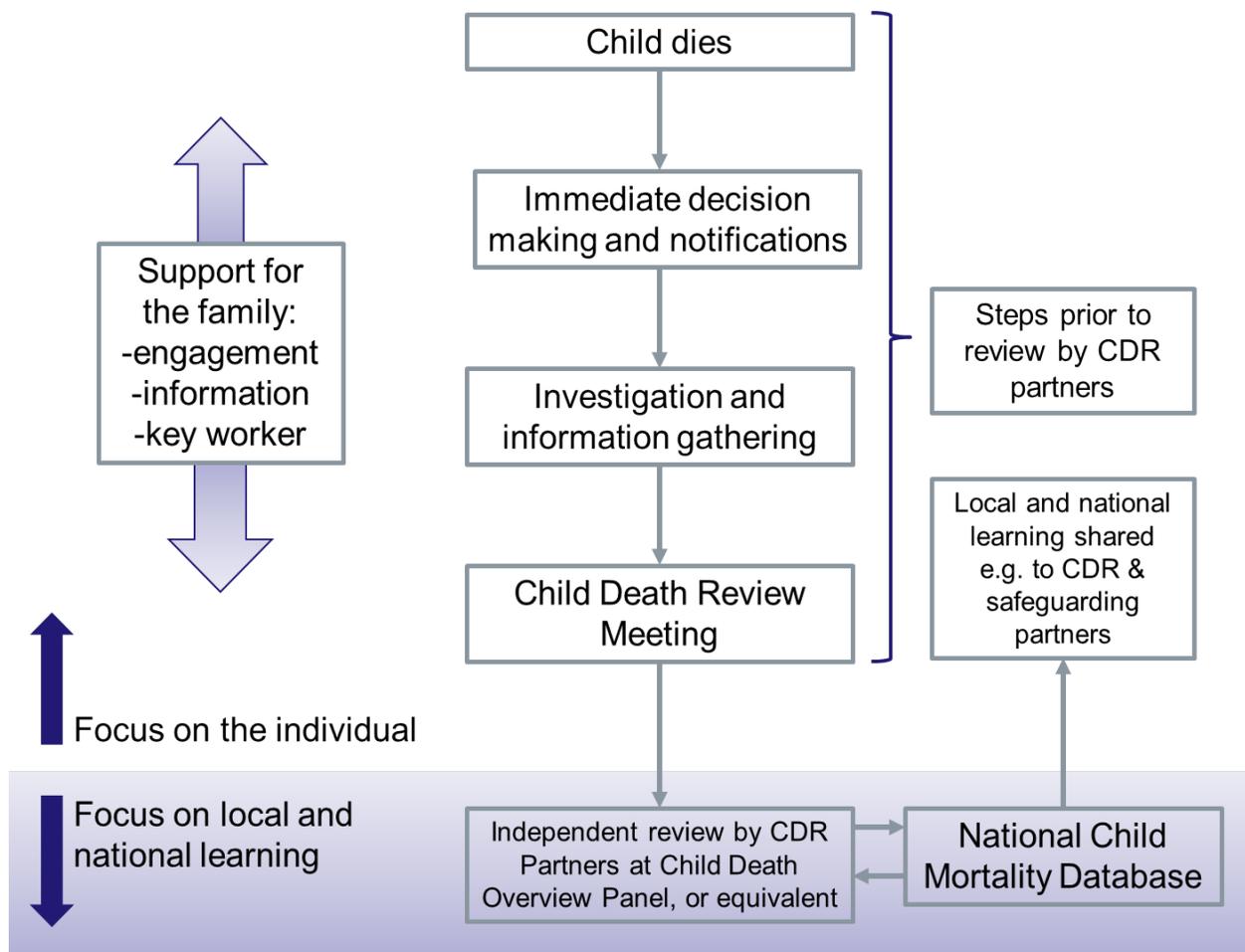


Figure 1. Chart illustrating the full process of a child death review. This includes both the statutory responsibilities of Child Death Review partners to review the deaths of children (described here as review at CDOP or equivalent), and the processes that precede or follow this independent review. Further explanation is below.

15. The *steps that precede* the child death review partners' independent review (figure 1), commence in the immediate aftermath of a child's death. These include the immediate decisions, notifications and parallel investigations, and the local case review by those directly involved with the care of the child or involved in the investigation after death, at the Child Death Review Meeting. The information gathered throughout this process should be fed into the partners' review.

16. The learning from all child death reviews should be shared with the National Child Mortality Database, once operational, which may in addition take into account information from other reviews in order to identify any trends or similarities with deaths. Information

from the database may be able to inform systematic or local changes to prevent future deaths. See paragraph 27 for transitional arrangements for the database.

17. The processes that should be followed by all those involved when responding to, investigating, and reviewing all child deaths is set out in the further guidance on child death reviews issued by the government.

18. All practitioners participating in the child death review process should notify, report, and scrutinise child deaths using the [standardised templates](#). These should be forwarded to the relevant CDOP (or other structure child death review partners have put in place to help review child deaths). The mechanism for collecting this data will evolve as the National Child Mortality Database becomes operational.

The child death review process

A child dies

19. Practitioners in all agencies should notify the local child death review partners, via the local CDOP administrator (or equivalent) of the death of any child of which they become aware by using the [notification](#) form.

Immediate decision making and notifications & Investigation and information gathering

20. Whenever a child dies, practitioners should work together in responding to that death in a thorough, sensitive and supportive manner. The aims of this response are to:

- establish, as far as is possible, the cause of the child's death
- identify any modifiable contributory factors¹⁰⁴
- provide ongoing support to the family
- learn lessons in order to reduce the risk of future child deaths and promote the health, safety and wellbeing of other children
- ensure that all statutory obligations are met

21. Where a Joint Agency Response is required, practitioners should follow the process set out in *Sudden and Unexpected Death in Infancy and Childhood: multiagency guidelines for care and investigation (2016)*. A Joint Agency Response is required if a child's death:

- is or could be due to external causes
- is sudden and there is no immediately apparent cause (including sudden

¹⁰⁴ These are defined as factors which may have contributed to the death of the child and which might, by means of a locally or nationally achievable intervention, be modified to reduce the risk of future deaths.

unexpected death in infancy/childhood)

- occurs in custody, or where the child was detained under the Mental Health Act
- occurs where the initial circumstances raise any suspicions that the death may not have been natural
- occurs in the case of a stillbirth where no healthcare professional was in attendance

22. If there is an unexplained death of a child at home or in the community, the child should normally be taken to an emergency department rather than a mortuary. In some cases when a child dies at home or in the community, the police may decide that it is not appropriate to move the child's body immediately, for example, because forensic examinations are needed.

23. In a criminal investigation, the police are responsible for collecting and collating all relevant information pertaining to the child's death. Practitioners should consult the lead police investigator and the Crown Prosecution Service to ensure that their enquiries do not prejudice any criminal proceedings.

24. If the results of any investigations suggest evidence of abuse or neglect as a possible cause of death, the paediatrician should inform relevant safeguarding partners and the Child Safeguarding Practice Review Panel immediately.

Child Death Review Meeting

25. This is the multi-professional meeting that takes place prior to the child death review partners review. At the meeting, all matters relating to an individual child's death are discussed by professionals involved with the case. The child death review meeting should be attended by professionals who were directly involved in the care of that child during his or her life and in the investigation into his or her death, and should not be limited to medical staff. A [draft analysis](#) form of each individual case should be sent from the child death review meeting to child death review partners to inform the independent review at a CDOP, or equivalent.

Review of death by child death review partners

26. The review by the child death review partners (at CDOP, or equivalent), is intended to be the final, independent scrutiny of a child's death by professionals with no responsibility for the child during their life. The information gathered using all the standardised templates may help child death review partners to identify modifiable factors that could be altered to prevent future deaths.

27. In addition to the statutory purposes set out above, the review should also provide

data¹⁰⁵ to NHS Digital and then, once established, to the National Child Mortality Database.

28. Child death review partners for a local authority area in England must prepare and publish a report as set out in the statutory responsibilities above. They may therefore wish to ask the CDOP (or equivalent) to produce an annual report for child death review partners on local patterns and trends in child deaths, any lessons learnt and actions taken, and the effectiveness of the wider child death review process in order to assist child death review partners to prepare their report.

¹⁰⁵ Specified data to NHS Digital for the transitional period will be notified to Child Death Review partners separately. The mechanism for collecting, and the content of, this data will evolve as the National Child Mortality Database becomes operational.

Appendix A: Glossary

Item	Definition
Children	Anyone who has not yet reached their 18th birthday. The fact that a child has reached 16 years of age, is living independently or is in further education, is a member of the armed forces, is in hospital or in custody in the secure estate, does not change their status or entitlements to services or protection.
Safeguarding and promoting the welfare of children	Defined for the purposes of this guidance as: <ul style="list-style-type: none"> a. protecting children from maltreatment b. preventing impairment of children's health or development c. ensuring that children are growing up in circumstances consistent with the provision of safe and effective care d. taking action to enable all children to have the best outcomes
Child protection	Part of safeguarding and promoting welfare. This refers to the activity that is undertaken to protect specific children who are suffering, or are likely to suffer, significant harm.
Abuse	A form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm, or by failing to act to prevent harm. Children may be abused in a family or in an institutional or community setting by those known to them or, more rarely, by others. Abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults, or another child or children.
Physical abuse	A form of abuse which may involve hitting, shaking, throwing, poisoning, burning or scalding, drowning, suffocating or otherwise causing physical harm to a child. Physical harm may also be caused when a parent or carer fabricates the symptoms of, or deliberately induces, illness in a child.

Item	Definition
Emotional abuse	<p>The persistent emotional maltreatment of a child such as to cause severe and persistent adverse effects on the child’s emotional development. It may involve conveying to a child that they are worthless or unloved, inadequate, or valued only insofar as they meet the needs of another person. It may include not giving the child opportunities to express their views, deliberately silencing them or ‘making fun’ of what they say or how they communicate. It may feature age or developmentally inappropriate expectations being imposed on children. These may include interactions that are beyond a child’s developmental capability, as well as overprotection and limitation of exploration and learning, or preventing the child participating in normal social interaction. It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyber bullying), causing children frequently to feel frightened or in danger, or the exploitation or corruption of children. Some level of emotional abuse is involved in all types of maltreatment of a child, though it may occur alone.</p>
Sexual abuse	<p>Involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example, rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children.</p>
Child sexual exploitation	<p>Child sexual exploitation is a form of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (a) in exchange for something the victim needs or wants, and/or (b) for the financial advantage or increased status of the perpetrator or facilitator. The victim may have been sexually exploited even if the sexual activity appears consensual. Child sexual exploitation does not always involve physical contact; it can also occur through the use of technology.</p>

Item	Definition
Neglect	<p>The persistent failure to meet a child’s basic physical and/or psychological needs, likely to result in the serious impairment of the child’s health or development. Neglect may occur during pregnancy as a result of maternal substance abuse. Once a child is born, neglect may involve a parent or carer failing to:</p> <ul style="list-style-type: none"> a. provide adequate food, clothing and shelter (including exclusion from home or abandonment) b. protect a child from physical and emotional harm or danger c. ensure adequate supervision (including the use of inadequate care-givers) d. ensure access to appropriate medical care or treatment <p>It may also include neglect of, or unresponsiveness to, a child’s basic emotional needs.</p>
Extremism	<p>Extremism goes beyond terrorism and includes people who target the vulnerable – including the young – by seeking to sow division between communities on the basis of race, faith or denomination; justify discrimination towards women and girls; persuade others that minorities are inferior; or argue against the primacy of democracy and the rule of law in our society.</p> <p>Extremism is defined in the Counter Extremism Strategy 2015 as the vocal or active opposition to our fundamental values, including the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. We also regard calls for the death of members of our armed forces as extremist.</p>
Young carer	<p>A young carer is a person under 18 who provides or intends to provide care for another person (of any age, except generally where that care is provided for payment, pursuant to a contract or as voluntary work).</p>
Parent carer	<p>A person aged 18 or over who provides or intends to provide care for a disabled child for whom the person has parental responsibility.</p>
Education, Health and Care Plan	<p>A single plan, which covers the education, health and social care needs of a child or young person with special educational needs and/or a disability (SEND). See the Special Educational Needs and Disability Code of Practice 0-25 (2014).</p>

Item	Definition
Local authority designated officer	<p>County level and unitary local authorities should ensure that allegations against people who work with children are not dealt with in isolation. Any action necessary to address corresponding welfare concerns in relation to the child or children involved should be taken without delay and in a coordinated manner. Local authorities should, in addition, have designated a particular officer, or team of officers (either as part of multi-agency arrangements or otherwise), to be involved in the management and oversight of allegations against people who work with children. Any such officer, or team of officers, should be sufficiently qualified and experienced to be able to fulfil this role effectively, for example qualified social workers. Any new appointments to such a role, other than current or former designated officers moving between local authorities, should be qualified social workers. Arrangements should be put in place to ensure that any allegations about those who work with children are passed to the designated officer, or team of officers, without delay.</p>
Safeguarding partners	<p>A <i>safeguarding partner</i> in relation to a local authority area in England is defined under the Children Act 2004 as: (a) the local authority, (b) a clinical commissioning group for an area any part of which falls within the local authority area, and (c) the chief officer of police for an area any part of which falls within the local authority area. The three safeguarding partners should agree on ways to co-ordinate their safeguarding services; act as a strategic leadership group in supporting and engaging others; and implement local and national learning including from serious child safeguarding incidents. To fulfil this role, the three safeguarding partners must set out how they will work together and with any relevant agencies as well as arrangements for conducting local reviews.</p>
Child death review partners	<p>A child death review partner in relation to a local authority area in England is defined under the Children Act 2004 as (a) the local authority, and (b) any clinical commissioning group for an area any part of which falls within the local authority area. The two partners must make arrangements for the review of each death of a child normally resident in the area and may also, if they consider it appropriate, make arrangements for the review of a death in their area of a child not normally resident there. They must also make arrangements for the analysis of information about deaths reviewed under this section. The purposes of a review or analysis are (a) to identify any matters relating to the death or deaths that are relevant to the welfare of children in the area or to public health and safety, and (b) to consider</p>

Item	Definition
	whether it would be appropriate for anyone to take action in relation to any matters identified.
County Lines	As set out in the Serious Violence Strategy , published by the Home Office, a term used to describe gangs and organised criminal networks involved in exporting illegal drugs into one or more importing areas within the UK, using dedicated mobile phone lines or other form of 'deal line'. They are likely to exploit children and vulnerable adults to move and store the drugs and money, and they will often use coercion, intimidation, violence (including sexual violence) and weapons.
Child criminal exploitation	As set out in the Serious Violence Strategy , published by the Home Office, where an individual or group takes advantage of an imbalance of power to coerce, control, manipulate or deceive a child or young person under the age of 18 into any criminal activity (a) in exchange for something the victim needs or wants, and/or (b) for the financial or other advantage of the perpetrator or facilitator and/or (c) through violence or the threat of violence. The victim may have been criminally exploited even if the activity appears consensual. Child criminal exploitation does not always involve physical contact; it can also occur through the use of technology.

Appendix B: Further sources of information

Department for Education guidance

- [Care of unaccompanied migrant children and child victims of modern slavery](#)
- [Child sexual exploitation: definition and guide for practitioners](#)
- [Children Act 1989: care planning, placement and case review](#)
- [Children Act 1989: court orders](#)
- [Children Act 1989: private fostering](#)
- [Information sharing: advice for practitioners providing safeguarding services](#)
- [Keeping children safe in education: for schools and colleges](#)
- [Knowledge and skills statements for child and family social work](#)
- [Listening to and involving children and young people](#) Department for Education and Home Office
- [Mandatory reporting of female genital mutilation: procedural information](#) Department for Education and Home Office
- [Multi-agency statutory guidance on female genital mutilation](#) Department for Education, Department of Health and Social Care, and Home Office
- [National action plan to tackle child abuse linked to faith or belief](#)
- [National minimum standards for private fostering](#)
- [Non-Maintained Special Schools Regulations 2015](#)
- [Pathways to harm, pathways to protection: a triennial analysis of serious case reviews, 2011 to 2014](#)
- [Preventing and tackling bullying](#)
- [Safeguarding children](#) Department for Education, Home Office, Ofsted, Department of Health and Social Care, Ministry of Housing, Communities & Local Government, Care Quality Commission, Department for Digital, Culture, Media & Sport, and Foreign & Commonwealth Office
- [Safeguarding Children in whom illness is fabricated or induced](#) Department for Education, Department of Health and Social Care and Home Office
- [Safeguarding children who may have been trafficked](#) Department for Education and Home Office
- [Safeguarding strategy - unaccompanied asylum seeking and refugee children](#)
- [Sexual violence and sexual harassment between children in schools and colleges](#)
- [Statutory framework for the early years \[under 5s\] foundation stage \(EYFS\)](#)
- [Statutory guidance on children who run away or go missing from home or care](#)

- [Statutory visits to children with special educational needs and disabilities or health conditions in long-term residential settings](#) Department for Education and Department of Health and Social Care.
- [The Child Safeguarding Practice Review and Relevant Agency \(England\) Regulations 2018](#)
- [The prevent duty: for schools and childcare providers](#)
- [United Nations Convention on the rights of the child](#)
- [Use of reasonable force in schools](#)
- [Visiting children in residential special schools and colleges](#) Department for Education and Department of Health and Social Care
- [What to do if you're worried a child is being abused: advice for practitioners](#)

Guidance issued by other government departments and agencies

- [Achieving Best Evidence in Criminal Proceedings: Guidance on interviewing victims and witnesses, and guidance on using special measures](#) Ministry of Justice
- [Advice to parents and carers on gangs](#) Home Office
- [Advice to schools and colleges on gangs and youth violence](#) Home Office
- [Apply for a forced marriage protection order](#) Foreign & Commonwealth Office
- [Arrangements to Safeguard and Promote Children's Welfare](#) (original title "Every Child Matters") UK Visas and Immigration
- [Asset Plus: assessment and planning in the youth justice system](#) Youth Justice Board
- [Carers Strategy: Second National Action Plan 2014-2016](#) Department of Health and Social Care
- [Carers Strategy: the second national action plan 2014-2016](#) Department of Health and Social Care
- [Channel Duty guidance - Protecting vulnerable people from being drawn into terrorism](#) Home Office
- [Criminal exploitation of children and vulnerable adults: county lines](#) Home Office
- [Cyber Aware](#) National Cyber Security Centre
- [DBS barring referral guidance](#) Disclosure and Barring Service
- [Developing local substance misuse safeguarding protocols](#) Public Health England
- [Disclosure and Barring Services](#) Disclosure and Barring Service
- [Female Genital Mutilation Protection Orders: factsheet](#) Home Office
- [Forced marriage](#) Foreign & Commonwealth Office and Home Office
- [Forced Marriage Protection Orders](#) HM Courts & Tribunals Service
- [Guidance for health professionals on domestic violence](#) Department of Health and Social Care

- [Handling cases of forced marriage: multi-agency practice guidelines](#) Foreign & Commonwealth Office
- [Indecent images of children guidance for young people](#) Home Office
- [Mental Health Act 1983 Code of Practice: Guidance on the visiting of psychiatric patients by children](#) Department of Health
- [Mental Health Act 1983 Code of Practice: Guidance on the visiting of psychiatric patients by children](#) Department of Health
- [Missing Children and Adults - A Cross Government Strategy](#) Home Office
- [Modern slavery Act statutory guidance](#) Home Office
- [Multi-agency public protection arrangements \(MAPPA\)](#) Ministry of Justice, National Offender Management Service, and HM Prison Service
- [National service framework: children, young people and maternity services](#) Department of Health and Social Care
- [NHS England safeguarding Policy](#) NHS England
- [Prison, probation and rehabilitation: Public protection manual](#) National Offender Management Service and HM Prison Service
- [Probation service guidance on conducting serious further offence reviews framework](#) Ministry of Justice
- [Radicalisation - Prevent strategy](#) Home Office
- [Recognised, valued and supported: next steps for the carers strategy 2010](#) Department of Health and Social Care
- [Safeguarding vulnerable people in the reformed NHS: Accountability and Assurance Framework](#) NHS England
- [Serious and Organised Crime Toolkit: An Interactive Toolkit for practitioners working with young people](#) Home Office
- [Thinkuknow \[Supporting children to stay safe online\]](#) National Crime Agency
- [Understanding the female genital mutilation enhanced dataset: updated guidance and clarification to support implementation](#) Department of Health and Social Care
- [Violence against women and girls](#) Home Office

Guidance issued by external organisations

- [Child maltreatment: when to suspect maltreatment in under 18s](#) NICE
- [Child protection and the Dental Team](#) British Dental Association
- [Children's Commissioner](#)
- [Children's rights and the law](#) - Children's Rights Alliance for England
- [Cyberbullying: Understand, Prevent, Respond – Guidance for Schools](#) Childnet International
- [How we protect children's rights](#) – Unicef

- [Inter parental relationships](#) Early Intervention Foundation
- [NICE guideline on child abuse and neglect](#) NICE
- [Prison and Probation Ombudsman's fatal incidents investigation](#)
- [Private fostering](#) CoramBAAF
- [Protecting children and young people: doctors' responsibilities](#) General Medical Council
- [Safeguarding Children Toolkit for General Practice](#) Royal College of General Practitioners
- [Standards for safeguarding and protecting children in sport](#) NSPCC
- [Sudden unexpected death in infancy and childhood: multi-agency guidelines for care and investigation](#) Royal College of Pathologists
- [Whistleblowing advice line](#) NSPCC
- [Working Together with Parents Network update of the DoH/DfES Good practice guidance on working with parents with a learning disability \(2007\)](#) University of Bristol



HM Government

© Crown copyright 2018

This publication (not including logos) is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

To view this licence:

Visit www.nationalarchives.gov.uk/doc/open-government-licence/version/3

Email psi@nationalarchives.gsi.gov.uk

write to Information Policy Team, The National Archives, Kew, London, TW9 4DU

About this publication:

enquiries: www.education.gov.uk/contactus

download www.gov.uk/government/publications

Reference: DFE-00195-2018



Follow us on Twitter:
[@educationgovuk](https://twitter.com/educationgovuk)



Like us on Facebook:
facebook.com/educationgovuk