A 10 step guide to sharing information to safeguard children

▶ Latest updates

Introduction

This is a 10 step guide on data protection considerations when sharing personal information for child safeguarding purposes. It aims to help you feel confident about sharing information when you need to safeguard a child or young person at risk of harm.

It does not tell you how to safeguard children and young people, but it does give you practical advice on data protection as part of the safeguarding process. The ICO's role is as the regulator of information rights, not of safeguarding practices.

Data protection law allows you to share information when required to identify children at risk of harm and to safeguard them from harm. Data protection law doesn't prevent you from doing this. It simply helps you to share information in a fair, proportionate and lawful way.

It can be more harmful not to share information that is needed to protect a child or young person.

Appropriate information sharing is central to effectively safeguarding children from harm and promoting their wellbeing. There have been many reviews of cases where children have died or been seriously harmed through abuse or neglect. The case reviews frequently identify gaps in information sharing as a factor contributing to failures to protect the children involved.

Data protection law has an enabling role, supporting you to share information.

Who is this guidance for?

This guide is aimed at people who are involved in safeguarding children: at all levels, and in all sectors in the UK.

Safeguarding children is everyone's responsibility – not just practitioners in child safeguarding.

The NSPCC emphasises:

> "If you have any concerns at all about a child's safety or wellbeing, don't hesitate to contact [the NSPCC]".

There is no single definition of safeguarding. Sharing information to safeguard children includes:

- preventing harm;
- promoting the welfare of a child; and
- identifying risk in order to prevent harm (especially helpful where the risk may not be obvious to a single person or organisation).

A number of organisations have their own definitions and advice on safeguarding (see the Annexe for definition examples).

In this guide, the 'safeguarding of children' and references to children include children and young people up to the age of 18.

The information in this guide is important for people in a wide range of roles and organisations, such as:

- senior leaders in organisations (they might not work directly with children on a day-to-day basis, although some have a legally defined role, such as Directors of Children's Services in England, and the Chief Social Work Officer in Scotland);
- managers who hold key responsibilities for ensuring their staff share information appropriately, and sit between senior leadership and people in front line practice;
- people who are designated safeguarding leads and practitioners, as well as people who are less directly involved;
- those who work or volunteer in smaller local organisations such as youth groups, arts groups, or sports teams, including the social sector;
- those who work in the private sector, such as childminders, private schools, private day nurseries, and after school clubs; and
- competent authorities, such as the police or certain other public bodies and specific officials, sharing personal information for law enforcement purposes, who are subject to Part 3 of the Data Protection Act 2018 (DPA 2018).

Senior leaders should make sure everyone in their organisation has the required level of understanding of what to do to safeguard children. See Step 3: Develop clear and secure policies and systems for sharing information for more on this.

Further reading

- What is a competent authority?
- Are we processing for law enforcement purposes?

Follow these 10 steps:

- Step 1: Be clear about how data protection can help you share information to safeguard a child.
- Step 2: Identify your objective for sharing information, and share the information you need to, in order to safeguard a child.
- Step 3: Develop clear and secure policies and systems for sharing information.
- Step 4: Be clear about transparency and individual rights.
- Step 5: Assess the risks and share as needed.
- Step 6: Enter into a data sharing agreement.
- Step 7: Follow the data protection principles.
- Step 8: Share information using the right lawful basis.
- Step 9: Share information in an emergency.
- Step 10: Read our data sharing code of practice.

Step 1: Be clear about how data protection can help you share information to safeguard a child

Our clear message is that data protection is a framework to help you share information. It doesn't prevent you from sharing information to safeguard a child.

It can be more harmful not to share information that is needed to protect a child or young person.

Example

In a hospital out-patients appointment, a doctor suspects that a carer has inflicted an injury on a child. The doctor follows procedures and does not hesitate to share information about the child and their injury with local safeguarding services.

But we know that there can be challenges when you want to share information:

- practical challenges, such as technological ones, or relating to systems and processes that aren't effective or that aren't compatible with other organisations you need to share information with;
- challenges due to organisational culture or long-established practices, that can be difficult to change; and
- misconceptions that you cannot share information 'due to data protection'. Yes, you can!

Following these steps will help you to overcome these.

Get advice from your data protection officer (DPO), expert or team about your information sharing plans. For smaller organisations, ask your umbrella group or governing body for advice.

There are likely to be other laws and duties outside data protection that you also have to comply with in your safeguarding work. Some of those require you to share information in certain circumstances. Some sectors have particular requirements; for example, guidance for professionals laid down by UK regulators such as the General Medical Council, which cover things such as doctor-patient confidentiality. For those detailed requirements within your own organisation, make sure you adhere to agreed policies and obtain internal advice as needed.

Also, don't worry about receiving a fine or other penalty, when you share information in good faith to help identify and safeguard a child you believe is at risk of harm. You won't get into trouble with us. It will never breach UK data protection law to share all the information you need to with an appropriate person or authority in order to safeguard a child.

The Information Commissioner has made this clear in his video message:

00:57

The ICO upholds information rights in the public interest, and we always use our powers in a targeted and proportionate way. Our focus is to help you carry out information sharing in a compliant way, to support child safeguarding.

Further reading

Data protection officers (DPOs)

Step 2: Identify your objective for sharing information, and share the information you need to, in order to safeguard a child

Be clear about your purpose for sharing the information.

Safeguarding a child is a compelling reason for sharing information.

You can share all the information you need to, with an appropriate person or authority, in order to safeguard a child.

How this works in practice

You are working with a child and have identified concerns about their welfare. You are going to share this information with an organisation who can help, and you want to know how much to share.

- You may be able to share a minimal amount of information to achieve your purpose, such as accessing direct support for a service to benefit the child. In this scenario, it's appropriate only to share this minimal information.
- However, there will be times where multiple organisations are involved in an intervention, or where there are concerns about serious harm. In these cases, it may be necessary to share information more widely, or to share more information on a child's circumstances.

It is not always clear how the details of a child's history or circumstances are relevant to the concerns you've identified. But you will be sharing proportionately if you can link it back to a compelling reason to share. In these circumstances, that compelling reason is safeguarding the child.

Documenting this link will not only help you make your decision, but it helps you comply with the law.

Further reading

- Principle (b): Purpose limitation
- Principle (c): Data minimisation
- Data sharing and children

Step 3: Develop clear and secure policies and systems for sharing information

Put strong governance, policies and systems in place and keep everything under regular review.

Follow a 'data protection by design and default' approach to handling and sharing information.

Build a culture of compliance and good practice throughout your organisation to help you to share information securely.

Train everyone in your organisation in safeguarding and data protection to the level they need. Ensure that staff, contractors and volunteers all understand what they need to do to share information to safeguard children.

Example

A nursery assistant notices a concerning pattern of behaviour by an adult towards a toddler in the adult's care. The nursery assistant understands that she needs to promptly tell her manager her concerns. To protect the child, the nursery shares the information with local safeguarding services.

If safeguarding is not their day-to-day responsibility, they will require additional support from their management team.

Arrange regular refresher sessions of this training.

Alongside your organisation's training, policies and procedures, highlight information on where people working within your organisation can get help on data protection, so they have support to make the right decisions.

Putting these policies and systems in place will help you to share information, whether you are sharing information on a routine basis or as a one-off.

Routine information sharing is sharing done on a regular basis in a pre-planned way. For example, a group of organisations might arrange to share information for specific purposes, on a frequent or regular basis, or both.

For this type of sharing, establish rules and agree procedures in advance, including assessing the risks by doing a DPIA and entering into a data sharing agreement.

For one-off information sharing, make a decision on what is needed to safeguard a child based on the circumstances at the time, bearing in mind what is fair and proportionate. Planning ahead within your organisation will make the process clear to everyone. However, in some instances you may decide, or be asked, to share information in one-off situations that are not covered by any routine arrangement or agreement. You may still share that information, assessing the risks at the time. We recommend that you make plans to cover such situations.

Sometimes you may have to decide quickly about sharing information in conditions of real urgency, or even in an emergency. In these situations, don't be put off from sharing information; assess the risk and do what is necessary and proportionate. (See Step: 9 Share information in an emergency).

Example

In a secondary school in north west England, a maths teacher was concerned about a young person, J, in her class as she had noticed that his mood had changed. This included J letting his head drop to the table instead of working and being unwilling to speak in front of others. This was out of character. The teacher expressed her concern via the school's online safeguarding system to the school's safeguarding lead.

The same day, J's form tutor also raised a concern via the school's online safeguarding system, saying he had noticed J seemed much more tired than usual. He had tried to get J to talk about it, but J was reluctant to engage - although J did say he was feeling sad.

Both concerns led to the pastoral manager speaking to J the same day. J became tearful and explained he was worried about how he was feeling, because he could not shake the sense of sadness and worry. J also disclosed that he had recently begun to self-harm, but it became clear that he had not experienced any suicidal thoughts.

The pastoral manager found out from J that he was feeling extremely anxious about his parents' divorce and his current housing situation. He was clear that there were no concerns about his parents.

The safeguarding officer phoned home to discuss the concerns with the family and agreed with the family that she would make a referral to CAMHS (Child and Adolescent Mental Health Service).

She drew up a safety plan with the young person and his family before the end of the day and, as the CAMHS referral was likely to take some time, arranged for the young person to begin to see the school's counsellor straight away.

She discussed the housing situation with the family and offered a referral to the local Families First support service. The family said they felt they did not need it at the present time; the officer arranged to check back in with them weekly.

Note that different devolved referral agencies and arrangements may be in place in Northern Ireland, Scotland and Wales.

Further reading

- Accountability
- Guide to accountability and governance
- Data protection by design and defaultData sharing covered by the code

Step 4: Be clear about transparency and individual rights

Be clear about what happens to personal information at every stage; about how you'll inform people about this, and how you'll handle requests by people to access their information rights.

Tell people about how and why their information is used, giving them privacy information.

In any sharing arrangement, ensure you have policies and procedures that allow people to exercise their individual rights under data protection law:

- the right to access information held about them (the right of subject access);
- the rights to have their information rectified, erased or restricted;
- the right to object;
- the right to portability of their information; and
- the right not to be subject to a decision based solely on automated processing.

However, if you're sharing information for safeguarding purposes, you might not be obliged to allow people to exercise all these rights. For example, if giving access to a person to information you hold about them would be likely to cause serious harm to a child.

There are exemptions and restrictions that you may use in some circumstances to limit these rights. The DPA 2018 lists the exemptions relating to health, social work, education and child abuse, and the circumstances where they can be applied. This includes cases of information being processed by a court, requests made by someone with parental responsibility or in cases where compliance would be likely to cause someone serious harm.

Further reading

- Fairness and transparency in data sharing
- The rights of individuals
- Exemptions

Step 5: Assess the risks and share as needed

When you are making a decision about sharing information about a child, it is very important to assess the risks.

If you are an organisation that shares information on a regular or routine basis, a Data Protection Impact Assessment (DPIA) will help you to do that. A DPIA is a practical tool to help you plan for the information sharing and assess and mitigate the risks to children's rights and freedoms. It helps you to ensure your sharing is done safely, lawfully and with accountability. You may decide to carry out an overarching DPIA to cover situations that occur on a regular basis. It is worth noting that all organisations involved in the sharing need their own DPIA.

To do a DPIA, ask your data protection officer (DPO), expert or team, and for smaller organisations, your umbrella group or governing body.

However, there will be circumstances not covered by a DPIA, such as sharing information on a one-off basis (for example, if you are an individual employee or volunteer raising the alarm over something you have seen), or in an urgent situation or in an emergency. You can go ahead and share that information based on what is necessary and proportionate in the circumstances at the time to safeguard the child.

Further reading

- Deciding to share data
- Data protection impact assessments
- Sample DPIA template
- Data sharing in an urgent situation or in an emergency

Step 6: Enter into a data sharing agreement

Although it isn't mandatory to enter into a data sharing agreement, we recommend it because it helps all parties.

As an organisation, draw up a data sharing agreement (DSA) between you and any others that you are intending to share information with. As with a DPIA this is more likely to be feasible in scenarios of regular and routine information sharing between organisations.

Benefits include helping you and the party or parties you are planning to share the information with to:

- be clear about what information you are sharing;
- be clear how it will happen; and
- demonstrate that you are responsible for complying with data protection law (the accountability principle).

It may also be known as an information sharing agreement (ISA), or a data or information sharing protocol or contract.

Some organisations, including Government departments, may instead enter into a memorandum of understanding (MOU) with each other that includes information sharing provisions and fulfils the role of a data sharing agreement.

Consult your DPO, expert or team, or for smaller organisations, your umbrella group or governing body about drawing up a data sharing agreement.

Example

Some local organisations wanted to identify young people who already had been or were currently at high risk of disengaging from education, employment or training. They decided to routinely share personal information with each other. These partner organisations included two councils, local schools and colleges, housing providers, relevant community organisations, the local job centres and careers service. By sharing the information, they were able to co-ordinate their approach to providing the most appropriate support to the young person to encourage them back into education, work or training.

The partners used a data sharing agreement to set out their purpose, lawful bases and the information they would share. The agreement included a section on how to handle people's rights and agreed shared security standards; the partners also updated their privacy notices. To quality-assure their agreement, they shared it with a regional group of data protection practitioners for feedback. They also set a timescale for the partners to regularly review the agreement to ensure it stayed up-to-date and fit for purpose.

Further reading

- Data sharing agreements
- Accountability

Step 7: Follow the data protection principles

The seven data protection principles lie at the heart of data protection; follow them when handling or sharing personal information. They are all important.

- Lawfulness, fairness and transparency
- Purpose limitation (share only for your clear, specified, legitimate purposes)
- Data minimisation (share information that is adequate, relevant and limited to what is necessary for your purposes)
- Accuracy (and keep the information up to date)
- Storage limitation (keep the information no longer than necessary for your purposes)
- Integrity and confidentiality (ensure appropriate security)
- Accountability (demonstrate your compliance with the principles)

Please note that the principles and some other provisions are slightly different for law enforcement processing under Part 3 of the DPA 2018.

Further reading

- Data protection principles
- Data protection by design and default
- Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the GDPR and Part 2 DPA 2018
- Law enforcement processing principles

Step 8: Share information using the right lawful basis

Sharing information is always lawful when you choose the right lawful basis for you and for the circumstances. The ICO has a tool to help you – see below.

A lawful basis is a valid reason in data protection law for processing personal information. Using the right lawful basis means you can share all the information you need to, with an appropriate authority or individual, in order to safeguard a child.

Identify at least one lawful basis for sharing information before you start the sharing. Ensure you can demonstrate that you considered which lawful basis to use, in order to satisfy the accountability principle. Keep a record of your decision and your reasons, even if you decide that you do not have a lawful basis and therefore can't share the information.

Consent is one lawful basis, but it is not required for sharing information in a safeguarding context. In fact, in most safeguarding scenarios you will be able to find a more appropriate lawful basis.

See more on this, below.

Example

A teacher notices a child in his class is demonstrating some concerning behaviour, including showing fear about being collected from school by a relative with whom they live. The teacher follows the school's procedures and speaks to the safeguarding lead. The school contacts the local safeguarding service to share the information about the child.

The school does not need to obtain the consent of the relative to share this information.

The most common lawful bases suitable for safeguarding purposes are public task, legitimate interests and legal obligation.

Further reading

Use the ICO's lawful basis interactive guidance tool to help you to choose the appropriate lawful basis for your sharing arrangement.

Public task: a lawful basis mainly for public sector organisations

This allows you to share information "in the exercise of official authority". 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 share information using public task, as long as you have a clear basis in law.

Further reading

Public task

Legitimate interests: a lawful basis for organisations outside the public sector

For example, charities or other social sector organisations, or the private sector. This includes organisations in the private or social sector contracted by a public authority to deliver a service.

Further reading

Legitimate interests

Legal obligation: where you're required by a different law to share information to safeguard a child

This might be a law outside data protection, and it might be either in statute or in common law, but not a contractual obligation.

Further reading

Legal obligation

Vital interests: sharing information to protect a life

Of course, you can always share information in an urgent situation where a child's life or immediate wellbeing might be at risk.

Further reading

Vital interests

Consent

While it is always good to work with the knowledge and understanding of those involved, or even their agreement, it is important to remember that the lawful basis of consent is not required for sharing information in a safeguarding context. And the withholding of consent will not affect your ability to share for a legitimate safeguarding purpose.

For a number of reasons, including the fact that there is often an imbalance of power between people and organisations, there is likely to be a different, more appropriate lawful basis for the information sharing.

Note

Please bear in mind that in data protection the lawful basis of consent has a technical meaning that is completely different and separate from any other type of consent, agreement or permission that you might need to obtain from someone as part of service provision. For example, consent to medical treatment.

Don't conflate them with the data protection lawful basis of consent, although we acknowledge that in practice there may be, or may appear to be, a degree of overlap.

Further reading

Consent

Additional rules for special category (sensitive) data

- For special category data there are more rules to meet. Special category data is personal information that is sensitive and therefore needs more protection. It includes information about health, or revealing racial or ethnic origin.

  When you are planning to share special category data, in addition to identifying a lawful basis, you also need to meet:
  - a condition for processing under Article 9 of the UK GDPR (including health and social care); and
  - for some of those provisions, a condition in the DPA 2018 (including substantial public interest conditions such as the safeguarding of children and individuals at risk).
- When sharing information to safeguard a child, in the light of all the other factors you have considered, you are very likely to be able to meet one or more conditions.
- Sharing sensitive data for law enforcement purposes under Part 3 of the DPA 2018 is slightly different.

Further reading

- Special category data
- Law enforcement processing principles

Step 9: Share information in an emergency

In an emergency, don't hesitate to share information to safeguard a child. You might not have time to follow all the usual processes.

Make a record of what you shared, who with, and why, as soon as possible.

Some situations might be urgent, but not an emergency. Take a proportionate approach in the circumstances.

Plan ahead for emergency or urgent situations so that everyone knows what to do and the processes to follow when time is of the essence.

Further reading

Data sharing in an urgent situation or in an emergency

Step 10: Read our data sharing code

We recommend you use this 10 step guide in conjunction with our:

- Data sharing code of practice
- Data sharing page

Annexe

Here are some examples of definitions of safeguarding:

NSPCC

> “What is safeguarding?
>
> Safeguarding is the action that is taken to promote the welfare of children and protect them from harm.
>
> Safeguarding means:
>
> - protecting children from abuse and maltreatment
> - preventing harm to children’s health or development
> - ensuring children grow up with the provision of safe and effective care
> - taking action to enable all children and young people to have the best outcomes.
>
> Child protection is part of the safeguarding process. It focuses on protecting individual children identified as suffering or likely to suffer significant harm. This includes child protection procedures which detail how to respond to concerns about a child.”

Department for Education - England

The Department for Education’s statutory ‘Working Together’ guidance for safeguarding and promoting the welfare of children defines safeguarding as:

> - “protecting children from maltreatment;
> - preventing impairment of children’s mental and physical 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.”

Education Scotland

The Education Scotland child protection and safeguarding policy says about safeguarding:

> “This is a much wider concept than child protection and refers to promoting the welfare of children, young people and protected adults. It encompasses protecting from maltreatment, preventing impairment of their health or development, ensuring that they are growing up in circumstances consistent with the provision of safe and effective care, and taking action

to enable all children, young people and protected adults to have the best outcomes. Child protection is part of this definition and refers to activities undertaken to prevent children suffering, or likely to suffer, significant harm.

We have a distinctive approach to safeguarding in Scotland linked to Getting It Right for Every Child (GIRFEC) which promotes action to improve the wellbeing of every child and young person."