



Department
for Education

Information Sharing

**Advice for practitioners providing
safeguarding services for children,
young people, parents and carers**

May 2024

Contents

The Seven golden rules for sharing information (including personal information):	4
Introduction	6
About this advice	6
Definitions (as defined in Working Together to Safeguard Children 2023)	6
What is this advice for?	6
Who is this advice for?	7
Understanding “safeguarding”	7
Understanding “information sharing”	8
The importance of sharing information	8
Why data protection legislation does not prevent information sharing	9
Understanding the term ‘lawful basis’	9
The lawful bases which are most relevant for practitioners working with children	9
Why consent is not usually the most appropriate lawful basis in a safeguarding context	10
The complexities of “consent” and why it causes confusion	11
How to share information and retain a trusted relationship with children and families	11
How the common law duty of confidentiality affects information sharing	12
How the Human Rights Act 1998 affects information sharing	13
Effective Information Sharing: Your Responsibilities	14
Information sharing responsibilities	14
Senior leader responsibilities	14
The importance of sharing information with colleagues outside of your agency or organisation	14
The importance of providing feedback to agencies or organisations about the information they have shared	15
The justification for sharing information to safeguard a child	15
Sharing information, including personal information, with other agencies or organisations	16
Data Sharing Agreements (DSA)	16
Data Protection Impact Assessments (DPIA)	16
Knowing the amount of information to share	16
Who to contact if you are unsure whether to share information	17
Informing the people whose information you have shared	17

Sharing information in an urgent or emergency situation	17
The benefits of sharing information early	18
Information seeking	19
Being alert to different forms of abuse and neglect and taking action	19
Where to report concerns about a child's safety	20
Annex A: Data Protection	21
The meaning of data protection	21
Data sharing code of practice	21
The data protection principles	21
The rights of individuals	22
Data protection definitions	23
Annex B: Useful resources and advice	27

The Seven golden rules for sharing information (including personal information):

- 1. All children have a right to be protected from abuse and neglect. Protecting a child from such harm takes priority over protecting their privacy, or the privacy rights of the person(s) failing to protect them.** The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) provide a framework¹ to support information sharing where practitioners have reason to believe failure to share information may result in the child being at risk of harm.
- 2. When you have a safeguarding concern, wherever it is practicable and safe to do so, engage with the child² and/or their carer(s), and explain who you intend to share information with, what information you will be sharing and why.** You are not required to inform them, if you have reason to believe that doing so may put the child at increased risk of harm (e.g., because their carer(s) may harm the child, or react violently to anyone seeking to intervene, or because the child might withhold information or withdraw from services).
- 3. You do not need consent to share personal information about a child and/or members of their family if a child is at risk or there is a perceived risk of harm.** You need a lawful basis³ to share information under data protection law, but when you intend to share information as part of action to safeguard a child at possible risk of harm⁴, consent may not be an appropriate basis for sharing. It is good practice to ensure transparency about your decisions and seek to work cooperatively with a child and their carer(s) wherever possible. This means you should consider any objection the child or their carers may have to proposed information sharing, but you should consider overriding their objections if you believe sharing the information is necessary to protect the child from harm.
- 4. Seek advice promptly whenever you are uncertain or do not fully understand how the legal framework supports information sharing in a particular case.** Do not leave a child at risk of harm because you have concerns you might be criticised for sharing information. Instead, find out who in your organisation/agency can provide advice about what information to share and with whom. This may be your manager/supervisor, the designated safeguarding children professional, the data protection/information governance lead (e.g., Data Protection Officer⁵), Caldicott Guardian, or relevant policy or legal team. If you work for a small charity or voluntary organisation, follow the NSPCC's safeguarding guidance.
- 5. When sharing information, ensure you and the person or agency/organisation that receives the information take steps to protect the identities of any individuals (e.g., the child, a carer, a neighbour, or a colleague) who might suffer harm if their details became known to an abuser or one of their associates.**

6. **Only share relevant and accurate information with individuals or agencies/organisations that have a role in safeguarding the child and/or providing their family with support, and only share the information they need to support the provision of their services.** Sharing information with a third party rarely requires you to share an entire record or case-file – you must only share information that is necessary, proportionate for the intended purpose, relevant, adequate and accurate.
7. **Record the reasons for your information sharing decision, irrespective of whether or not you decide to share information.** When another practitioner or organisation requests information from you, and you decide not to share it, be prepared to explain why you chose not to do so. Be willing to reconsider your decision if the requestor shares new information that might cause you to regard information you hold in a new light. When recording any decision, clearly set out the rationale and be prepared to explain your reasons if you are asked.

¹ Where processing or sharing personal data, you must follow [the Information Commissioner's Code of Practice for Data Sharing](#) which should be read alongside the [ICO's guide to GDPR](#)

² Engagement with a child where it is appropriate to be based on their level of assessed competency. See [Gillick competence and Fraser guidelines | NSPCC Learning](#)

³ [Lawful basis for processing | ICO](#)

⁴ See page 9 of this document for further advice on appropriate lawful basis or use the [Lawful basis interactive guidance tool | ICO](#).

⁵ [Data protection officers | ICO](#)

Introduction

About this advice

This HM Government advice outlines the importance of sharing information about children, young people and their families in order to safeguard children. It should be read alongside the statutory guidance *Working together to safeguard children 2023*⁶. The advice is non-statutory and replaces the HM Government *Information sharing: advice for practitioners providing safeguarding services to children, young people, parents and carers* published in July 2018.

This advice focuses on the legal framework and how it supports information sharing for the purposes of safeguarding children from abuse and neglect. It does not detail the additional professional responsibilities that might apply for different practitioners. Practitioners should consider this advice alongside guidance specific to their profession or service area. For example, doctors should consider the General Medical Council guidance, *'Protecting Children and Young People'*⁷ and those working in schools and colleges should consider *Keeping Children Safe in Education*⁸. Other relevant guidance documents, such as the *Eight Caldicott principles*⁹, and useful materials can be found in Annex B.

Definitions (as defined in Working Together to Safeguard Children 2023)

A **child** is defined as anyone who has not yet reached their 18th birthday. 'Children' therefore means '**children and young people**' throughout the Advice.

We use the term '**practitioners**' in this Advice to include all individuals who work with children, young people and their families in any capacity.

What is this advice for?

The purpose of this advice is to:

- instil confidence in practitioners that the legal framework supports the sharing of information for the purposes of safeguarding
- provide a straightforward guide to practitioners on the core principles of timely and effective information sharing, that can be applied to day-to-day decision making

⁶ [Working together to safeguard children 2023: statutory guidance \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/115122/working-together-to-protect-children-2023.pdf)

⁷ [Protecting children and young people: The responsibilities of all doctors - ethical guidance summary - GMC \(gmc-uk.org\)](https://www.gmc-uk.org/ethical-guidance/ethical-guidance-summaries/protecting-children-and-young-people-the-responsibilities-of-all-doctors-ethical-guidance-summary.pdf)

⁸ [Keeping children safe in education 2023 \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/115122/keeping-children-safe-in-education-2023.pdf)

⁹ [Eight Caldicott Principles 08.12.20.pdf \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/115122/eight-caldicott-principles-08.12.20.pdf)

- support organisations to develop processes, policies and training for their practitioners based on this guide

The advice aims to promote and enable improved information sharing, to:

- identify, assess and respond to risks or concerns about the safety and welfare of children and young people in a timely and effective way
- join up “pieces of the jigsaw” for practitioners, so a true picture of what is happening in a child’s life can be understood
- assist children and families to receive support from across local agencies or organisations that meets their needs
- strengthen joined up working between practitioners and agencies or organisations, by removing perceived barriers to information sharing through a collective understanding about when and how information can be lawfully shared in the interests of a child

Who is this advice for?

This advice is for:

- all individuals who are directly involved in safeguarding children, including frontline practitioners, managers and senior leaders
- individuals and organisations that work with children, parents, carers and families, in sectors such as social care, education, health, justice and voluntary

It is vital to join up adult and children’s services for the purposes of safeguarding. Therefore, this advice may also be helpful for practitioners working with vulnerable adults and adults who could pose a risk to children.

Understanding “safeguarding”

For the purposes of this advice, we are drawing on the definition set out in Working Together to Safeguard Children 2023 as follows:

- providing help and support to meet the needs of children as soon as problems emerge
- protecting children from maltreatment, whether that is within or outside the home, including online
- preventing impairment of children’s mental and physical health or development
- ensuring that children are growing up in circumstances consistent with the provision of safe and effective care
- promoting the upbringing of children with their birth parents, or otherwise their family network through a kinship care arrangement, whenever possible and where this is in the best interests of the children

- taking action to enable all children to have the best outcomes in line with the outcomes set out in the Children's Social Care National Framework¹⁰

This advice focuses on the sharing of information where there are safeguarding concerns about a child. A concern could be based on an established risk (e.g. where there is evidence that a child has suffered harm) or a suspected or potential risk (e.g. where it is reasonable for a practitioner to believe that information sharing is necessary to protect a child from harm that may happen without intervention). It may be that the risk of harm to a child can only be identified and understood through the early sharing of concerns between practitioners and agencies or organisations who may hold relevant information about the child and can support action to safeguard the child.

Understanding “information sharing”

Information sharing in a safeguarding context means the appropriate and secure exchange of personal information, between practitioners and other individuals with a responsibility for children, in order to keep them safe from harm.

This advice relates to sharing case-level information about individual children and, where necessary, information about family members and other people who might – through their actions or neglect – put a child at risk of harm. This includes informal sharing of information between practitioners to develop an accurate understanding of a child or family, and more formal processes of sharing information such as referrals into local authority children's services. The principles of this advice may also be helpful to agencies or organisations managing larger scale sharing of child and family data, such as collation of data for development of local Joint Strategic Needs Assessments; however, this type of sharing is not the focus of this advice.

The importance of sharing information

Information sharing is essential for identifying patterns of behaviour, or circumstances in a child's life that may be evidence that they are at risk of harm or are being harmed and need some form of support or protection.

This includes but is not limited to:

- child abuse, neglect or exploitation
- situations where timely supportive intervention could prevent concerns about a child's wellbeing from escalating
- when a child is at risk of going missing or has gone missing
- when multiple children appear linked to the same risk
- where there may be multiple local authorities and agencies or organisations involved in the care of a child's care

¹⁰ [Children's social care: national framework - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/publications/children-social-care-national-framework)

Why data protection legislation does not prevent information sharing

Data protection legislation (the Data Protection Act 2018 (the DPA 2018) and UK General Data Protection Regulation (UK GDPR)) **does not** prevent the sharing of information for the purposes of safeguarding children, when it is necessary, proportionate and justified to do so. In fact, data protection legislation provides a framework which enables information sharing in that context. The first and most important consideration is always whether sharing information is likely to support the safeguarding of a child.

The ICO's *A 10 step guide to sharing information to safeguard children* summarises data protection considerations when sharing personal information for child safeguarding purposes.¹¹

Understanding the term 'lawful basis'

Under data protection law, you must have a valid lawful basis¹² in order to share personal information. You must identify at least one lawful basis under Article 6 of the UK GDPR for sharing. You can use the Information Commissioner's Office's (ICO) Lawful Basis Interactive Tool¹³, the ICO's 10 step guide or refer to the definitions in Annex A of this guidance for more help on this.

The lawful bases which are most relevant for practitioners working with children

There are six lawful bases¹⁴ for sharing information set out in Article 6 of the UK GDPR. No single basis is 'better' or more important than the others and the basis most appropriate to use will depend on the type of organisation you work for, your purpose for sharing and the nature of your relationship with the individual whose information you are sharing. Where there is an expectation on the part of the child or family that the common law duty of confidentiality applies, practitioners will need to consider the lawful basis for setting this aside, prior to making the decision about sharing information.

If you work in a public sector organisation, it is likely that "public task" or "legal obligation" will be the most appropriate lawful basis for you to use when sharing information to safeguard or protect the welfare of a child (e.g. when exercising statutory duties in relation to children under the Children Acts of 1989 and 2004 and other related legislation).

¹¹ [A 10 step guide to sharing information to safeguard children | ICO](#)

¹² [Lawful basis for processing | ICO](#)

¹³ [Lawful basis interactive guidance tool | ICO](#)

¹⁴ [A guide to lawful basis | ICO](#)

If you work with children and their families within the voluntary or private sectors, where your task, function or power does not have a clear basis in law, it is likely that the lawful basis of using “legitimate interests” may be more appropriate. (Refer to ‘Step 8: Share information using the right lawful basis’ of the ICO ten step guide for more information.)

Where the information to be shared is “special category data¹⁵” it will also be necessary to find a condition for processing the information under Article 9¹⁶ of the UK GDPR. Safeguarding of children and individuals at risk is one of the substantial public interest conditions under which the sharing of special category data may be authorised under Article 9. Further guidance on the processing of special category data is available on the ICO website¹⁷.

You can be confident in sharing personal information knowing that legislation allows you to share for safeguarding purposes

Why consent is not usually the most appropriate lawful basis in a safeguarding context

Consent should not be seen as the default lawful basis for sharing personal information in a child safeguarding context, as it is unlikely to be appropriate in most cases. The UK GDPR sets a high standard for consent to be used as a lawful basis; it must be specific, freely given, unambiguous, time limited and capable of being withdrawn by the individual at any time.

Using consent as a lawful basis means an individual has given agreement for personal information about themselves, or their child’s personal information, to be shared or processed for a purpose where they have a clear choice about its use. It also means that the individual is able to withdraw their consent at any time (in which case the information would need to be deleted).

These conditions are unlikely to be present in situations where practitioners are often under a professional duty to record information – irrespective of the wishes of the child or their family – in order to justify the decisions and actions they take in relation to the child’s needs, and where the overarching consideration will be whether information needs to be shared to safeguard a child where there is an established or potential risk of harm. Additionally, in some circumstances, seeking consent from a person you believe is neglecting or abusing a child is likely to undermine safeguarding procedures and may increase the risk of harm to the child or another person.

¹⁵ Special category data is defined in Annex A

¹⁶ [What are the conditions for processing? | ICO](#)

¹⁷ [Special category data | ICO](#)

It's important to get the lawful basis right. The legal framework can appear complex, and a lack of clarity can lead practitioners to assume, incorrectly, that no information can be shared because consent has not been provided. Don't let this happen; ensure you understand the correct lawful basis to use

The complexities of “consent” and why it causes confusion

The meaning attached to the term “consent”, and the expectations that it sets for how people make decisions, can be different depending on the context and how people are used to working within a particular environment. If these different meanings and expectations are conflated and confused, they can act as a barrier to appropriate information sharing when decisions have to be made about sharing information for safeguarding purpose. Some meanings attached to “consent” include:

- **“consent” as a lawful basis to share information**, as defined by data protection legislation (and relevant for the purpose of this Advice), is different to the general meaning of consent – such as the giving of permission. As already discussed, this is not usually the appropriate legal basis for sharing information to safeguard children
- **“consent” or “agreement” to receive a service**, such as a parent’s agreement to engage with services under section 17 of the Children Act 1989

The meaning of 'consent' in this context is the general sense of the word and is separate from the meaning of 'consent' as a lawful basis under data protection law. It may be necessary to share information even if the threshold for service intervention (for example, under s.17 of the Children Act 1989) has not been reached or where a person does not agree to the provision of particular services

- **“consent” to receive medical treatment**, there are specific meanings of implied and explicit consent for health purposes. Health practitioners should refer to their regulator’s guidance or NHS advice
- **being upfront, transparent and honest** with children and families. This is generally good practice, whenever it is safe to do so, as is emphasised throughout this advice (including below). This does not equate to obtaining “consent” from individuals to share their information (or information about their child) for data protection purposes, but this practice does promote engagement and collaboration

How to share information and retain a trusted relationship with children and families

Trusted relationships are at the heart of working with children and families. It is always good practice to work in partnership with children and families, communicating effectively and listening well, so that you have sufficient information to understand and be able to meet their needs. This openness is also important when deciding whether to share

information with other people, agencies or organisations about the children and families you are working with. If they have a choice about whether and how their information is shared or used, you should make this clear to them.

If you have concerns about a child's safety or welfare, and you are considering contacting support services about providing them or their parent(s) or carer(s) with specific support; being upfront, transparent, and honest about your concerns can give children the confidence to open up. It may also increase a parents' or carers' willingness to engage with services that provide family support.

If you have concerns about a child's safety and have decided to share information to protect them from a risk of harm, whenever it is safe and practical to do so, you should engage with the child, their parent(s) or carer(s) and explain who you intend to share information with, what information you will be sharing and why. This is unless seeking to discuss a potential concern would put the child or others at risk of harm.

If you have a professional or legal duty to share certain information, and the child or carer therefore does not have a choice about information sharing, they should still be informed about what information sharing has taken place and how the information will be used, wherever possible and safe to do so. However, you should not inform the child or their parent or carer about your decision to share information if doing so could put a child or others at further risk of harm, or could compromise effective safeguarding arrangements, including police investigations.

In any situation where children or their parent(s) or carer(s) object to particular information sharing, but you decide that nonetheless it is appropriate to share, you must record your reasons and the legal basis for doing so.

How the common law duty of confidentiality affects information sharing

The common law duty of confidentiality applies when an individual shares personal information with you in the expectation that this information will be kept confidential.

Under the common law, if you believe it is necessary to share confidential information, then you must be sure that one of the following conditions exists:

- You are legally required to share information (e.g. because legislation or a court order mandates information sharing)
- You believe there is an overriding public interest that justifies sharing information (e.g. where the sharing is necessary for safeguarding purposes) which outweighs the public interest in maintaining confidentiality, and the sharing of information is proportionate i.e. you only share the minimum amount of information necessary to assist another practitioner or organisation in protecting a child

Decisions about sharing confidential information should be taken on a case-by-case basis.

In situations where there is **not** a concern for the child's safety, the position is slightly different. For example, this might be the case in a situation when you consider a family would benefit from additional support to promote the welfare of their child. In such

situations you will usually need to gain consent from the child, their parent or carer to share confidential information.

If you are not sure if there is a concern for the child's safety or welfare, you should exercise your professional curiosity to find out as much as possible about the child to determine risk, before deciding on the most appropriate approach. If you are not able to determine an accurate understanding of a possible risk without sharing concerns with others, you should share the relevant information with those who need to know.

Practitioners should consider guidance from their professional regulator, agency or organisation as appropriate, or speak with their manager or supervisor, designated safeguarding children professional or information governance lead for detail on any specific confidentiality requirements. This is in addition to considering data protection requirements. Further information about the common law duty can be found in the NHS Transformation Directorate guidance 'Use and share information with confidence.'¹⁸

How the Human Rights Act 1998 affects information sharing

The Human Rights Act 1998 incorporates certain rights and freedoms guaranteed under the European Convention on Human Rights (ECHR) into domestic law. Human rights concerns, especially in light of the right to respect for a person's privacy and family life (Article 8¹⁹ of the ECHR), can sometimes be seen as a barrier to sharing information. However, where sharing of personal information is necessary to protect a child from harm, is proportionate and complies with data protection legislation, the sharing of that information is also likely to comply with the Human Rights Act.

¹⁸ [Use and share information with confidence - NHS Transformation Directorate \(england.nhs.uk\)](https://www.england.nhs.uk/our-work/using-information-to-improve-services/)

¹⁹ [Article 8 of the European Convention of Human Rights sets out the right to respect for private and family life.](#)

Effective Information Sharing: Your Responsibilities

Information sharing responsibilities

Everyone must take responsibility for sharing information in order to keep children safe from harm, they must not assume someone else will pass on information.

It is for local safeguarding partners²⁰ to consider how they will build positive relationships with other local agencies or organisations (which may cross geographical borders) to ensure that relevant information is shared in a timely and proportionate way.

Senior leader responsibilities

Senior leaders of organisations and agencies with safeguarding responsibilities should:

- Create an environment where practitioners feel confident about when and how to share information if a child is at risk or perceived risk of harm
- Ensure robust information sharing arrangements are in place, that – where necessary - data protection impact assessments have been carried out, and practitioners are supported to understand local information sharing processes and procedures including data safeguarding measures to ensure scrutiny and accountability on how data is requested, shared and stored
- Work with senior leaders in partner organisations to establish secure and effective systems and environments for sharing information
- Provide information materials to children and their families that ensure transparency around information sharing for safeguarding purposes and explain how individuals can exercise their rights
- Ensure practitioners have been trained to understand information governance and sharing arrangements, who they can contact in their organisation for advice, and where to direct children and their families should they need additional advice

The importance of sharing information with colleagues outside of your agency or organisation

It is likely that practitioners working in different agencies or organisations that have contact with children and their families will only have a partial view of what is happening in their lives. Sharing information helps to build up a fuller picture and is therefore an intrinsic part of any practitioner's job when working with children and families. Similarly, it is also important to share information with agencies that may be formulating a risk assessment about whether a particular individual poses a risk to children.

²⁰ A *safeguarding partner* in relation to a local authority area in England is defined under [s.16E of the Children Act 2004](#)

Decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. If you have concerns about a child, it is important to act on those concerns.

The most important consideration is whether the sharing of information is likely to support the safeguarding of a child

The importance of providing feedback to agencies or organisations about the information they have shared

When attempting to safeguard a child, practitioners should act in accordance with local procedures and, unless there is a sound reason not to, they should provide timely feedback²¹ on decisions taken following information being shared, to 'close the loop' with the professional who shared the information. Feedback can help encourage dialogue and develop a better understanding of when and what to share. A lack of feedback can contribute to a hesitancy to share information in the future.

Sharing information across agencies helps to piece together the “jigsaw pieces” of the child’s life and identify risks early

The justification for sharing information to safeguard a child

Sharing information for safeguarding purposes can be justified solely based on preventing harm to a child. The sharing of this information is not dependant on any thresholds for intervention. For example, it is not necessary for a formal process under section 17 or section 47 of the Children Act 1989 to be invoked in order for information to be shared, provided that the sharing is necessary for organisations and agencies to safeguard a child at possible risk of harm. It is only through sharing information that agencies or organisations and practitioners build a richer picture of the day-to-day life of the child and family they are working with.

Have confidence to share information – trust your instincts and act on your training, experience and risk assessment skills. Seek guidance if in doubt

²¹ Feedback on referrals to the local authority children's social care is outlined at Page 58, para 151 of [Working Together 2023](#)

Sharing information, including personal information, with other agencies or organisations

It's essential to plan ahead and have systems and procedures in place for sharing personal information, and for the management of that information. Know in advance which agencies or organisations you are able to share safeguarding information with and what they can do with the information. Seek advice whenever you are uncertain.

Data Sharing Agreements (DSA)

It is good practice for agencies or organisations to have in place DSAs²² with agencies or organisations with which they will be sharing information regularly. DSAs are also known as information sharing agreements (ISAs) or protocols.

Data Protection Impact Assessments (DPIA)

It is not usually necessary to undertake a DPIA²³ for sharing information on a one-off basis. However, before sharing any personal information on a regular basis, as part of a routine or planned sharing exercise, you or your agency or organisation should carry out a DPIA. For more information you can refer to Step 5 of the ICO's 10 step guide.

Knowing the amount of information to share

The sharing of personal information must be necessary, fair and proportionate – only share the personal information that is adequate, relevant and limited to what is necessary to protect a child from harm. Requests to share information should explain clearly what is required and why, clarifying any meaning or terminology where needed to avoid misinterpretation or misunderstanding. If in doubt about what information is needed, always seek clarification from the requesting agency or organisation.

Where you have concerns about a child and are unsure if they are at risk of harm, be open to contacting other practitioners who have contact with the child and sharing limited information with them, to see if they hold additional information which gives cause to believe the child is at risk of harm.

Information must always be shared securely. If you are unsure how to send or share information securely you should contact your manager, IT team or designated data protection or information governance lead (e.g., Data Protection Officer) to determine the correct route within your agency or organisation.

²² [Data sharing agreements | ICO](#)

²³ [Data Protection Impact Assessments \(DPIAs\) | ICO](#)

Any information which you think could safeguard a child should be shared with relevant agencies or organisations

Who to contact if you are unsure whether to share information

Practitioners should use their judgement when making decisions about what information to share, and the agency or organisation you work for should have policies and processes in place to ensure the safe and effective sharing of personal information for safeguarding purposes.

When in doubt about a decision to share personal information, seek advice. This could be from your manager or supervisor, agency or organisation's designated safeguarding children professional, the data protection or information governance lead (e.g., Data Protection Officer), Caldicott Guardian, professional regulator (if applicable) or your organisation's relevant policy or legal team.

Informing the people whose information you have shared

If it is safe to be transparent, be as open and honest as possible with the individual (and, or their family) from the outset and seek to work cooperatively with them. You should try to engage with the child and, or their carer(s), and explain who you intend to share information with, what information you will be sharing and why.

However, it is not always safe or appropriate to notify individuals that you intend to share their personal information. For example, you should not notify individuals if you have reason to believe that doing so may put the child at increased risk of harm. Likewise, in urgent cases, where a child is at immediate risk of harm, the priority is to share information quickly to protect the child, regardless of whether the relevant individual(s) have been informed.

While you do not have to rely upon consent as the lawful basis for sharing information, you must make information sharing decisions on a case-by-case basis. Where a child or their carer objects you should consider their objection but still share information if you believe it is necessary to protect the child from harm.

Sharing information in an urgent or emergency situation

Urgent or emergency situations can arise that you may not have envisaged, and you may have to deal with them on the spot. In an emergency where you consider there is a risk of harm to a child, you should go ahead and share information as is necessary and proportionate. Delays in sharing information may increase the risk of harm to the child. You must always document the action you took after the event if you cannot do it at the time, including recording a clear rationale for your decision. For further information see

the ICO Statutory Data Sharing Code of Practice²⁴ which contains guidance on sharing in an urgent situation or in an emergency.

The benefits of sharing information early

Practitioners should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety of children, whether this is when problems are first emerging (e.g. persistent school absences), 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).

In some circumstances, it may be possible to consider and refer the family to a range of early help and support they could access in the local area to address evolving concerns and before there is an impact on the child's overall safety. However, where a referral to these services is not necessary to protect a child from harm, you should generally seek the family's consent before doing so.

Sharing and acting on that information early, helps to ensure that a child and their family, receive the right services at the right time and helps to prevent a risk or need from becoming more acute. You or your agency or organisation may hold the key information in the jigsaw that confirms or corroborates the safeguarding risk.

Practitioners should be proactive in sharing their concerns about new or evolving risks impacting on a child's safety. Who you share information with should be guided by your local safeguarding arrangements and procedures. It is important and necessary to ensure information shared is relevant, timely, of sufficient quality and accurate.

It is often necessary to share small pieces of information regularly and proactively so that practitioners can build a picture of what is happening in a child's life

Practitioners should also be alert to the potential need to share important information about any adults with whom that child has contact, where it is reasonable to believe that their actions or neglect may cause harm to a child. Data protection law does not prevent you from doing that, when it's necessary, fair and proportionate, and provides a framework to help you to do so²⁵.

While it is essential to ensure that there is a lawful basis in data protection law for sharing information about adults related to or linked to the child, as stated earlier consent is unlikely to be the appropriate one to use. It's also important to note that it will not be appropriate to inform those adults if doing so will increase the risk of a child suffering harm.

²⁴ [Data sharing: a code of practice | ICO](#)

²⁵ See pages 5-8 of this advice for more detail on data protection law.

Information seeking

Practitioners should be proactive and should seek out relevant information from other practitioners and agencies or organisations to build an accurate picture of a child and family's life. Effective information seeking enables pieces of information to be shared, gathered, and triangulated across agencies or organisations working with a child and family.

Practitioners should be professionally curious about the information they hold, and the information other practitioners may hold about a child. This may involve checking with agencies to build a fuller understanding of a family's context or the risks of harm. You should be responsive to practitioners seeking information and share relevant information with practitioners when it supports the safeguarding of a child.

Being alert to different forms of abuse and neglect and taking action

All practitioners should be alert to the signs and triggers of abuse and neglect. Children may be vulnerable to neglect, abuse or exploitation from within their family and, or from individuals or peers they come across in their day-to-day lives. Sharing small pieces of information can help to build a fuller picture over time or can help to fill gaps in information to form a better understanding of the child or family's life. Abuse and neglect can take a variety of different forms, including but not limited to:

- sexual abuse
- physical abuse
- emotional abuse
- neglect (i.e., a child might be left hungry or dirty, or without proper clothing, shelter, supervision, health care or denied their right to education)
- domestic abuse, including controlling or coercive behaviour
- exploitation by criminal gangs and organised crime groups
- serious or physical violence (i.e., knife and gun crime)
- trafficking and modern slavery
- online abuse
- child on child abuse
- sexual exploitation
- female genital mutilation
- influences of extremism leading to radicalisation
- exposure to parental mental health issues; and
- drug or alcohol abuse

Whatever the form of abuse or neglect, practitioners should put the needs of children first when determining what action to take.

Children may report experiences of abuse or neglect to trusted adults, such as teachers, youth workers or sports coaches, or there may be visible signs of abuse or neglect, in which case the decision to share information is clear. Action should be taken quickly to respond to the report or signs. In other cases, e.g., neglect, the indicators may be subtle and appear or build up over time. In these cases, the situation can often be more difficult

to judge, however action should still be taken, and you should report concerns in line with safeguarding policies and procedures.

Everyone should be aware of the potential for children to be sexually or criminally exploited for money, power, or status, including child-on-child abuse, and practitioners should adopt an open and inquiring mind about the potential underlying reasons for behaviour changes in children of all ages. There will be occasions when children do not realise or recognise that they are being abused or exploited.

Where to report concerns about a child's safety

If a practitioner has concerns about a child's safety, they should share the information with local authority children's services in line with local procedures. Concerns about any child, including children who may already have a social worker, should be shared. Every organisation or agency should have clear guidance on how and when to do this.

Reporting concerns through a multi-agency referral for social care intervention may not always be the most suitable course of action. If the practitioner considers it to be a low-level concern, it may be more appropriate to report through the local early help process.²⁶

Security of information must always be considered and should be proportionate to the sensitivity of the information being shared and the circumstances of the concern.

²⁶ [Working together to safeguard children 2023: statutory guidance \(publishing.service.gov.uk\)](#) -Section 1, Page 44

Annex A: Data Protection

The meaning of data protection

Data protection law ensures the fair and proportionate use of information about people. It helps to build trust between people, organisations and businesses, and makes sure that people trust you to use and share their data fairly and responsibly.

All agencies or organisations should have policies and procedures in place which set out clearly the systems and processes and the principles for sharing information internally. In addition, these policies should cover sharing information with other agencies or organisations and practitioners, including third party providers to which local authorities have chosen to delegate children's social care functions, local safeguarding partners, and government agencies.

Data sharing code of practice

The Information Commissioner's Office (ICO) has produced a statutory data sharing code of practice²⁷. The code is published on the ICO's data sharing information hub²⁸ which also contains a range of other data sharing resources. The code is designed to provide practical guidance for organisations in all agencies or sectors about how to share personal information in compliance with data protection law. It aims to give confidence to share data fairly and proportionately.

The data protection principles

Article 5 of the UK GDPR sets out seven key principles²⁹ which lie at the heart of the general data protection regime. The UK GDPR principles are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

If you work for a competent authority such as the police or certain other public bodies and specific officials, when sharing data for law enforcement purposes³⁰ you need to consider Part 3 of the Data Protection Act 2018. Part 3, Chapter 2 of the Data

²⁷ [data sharing code of practice](#)

²⁸ [data sharing information hub](#)

²⁹ [The principles | ICO](#)

³⁰ [Scope and key definitions | ICO](#)

Protection Act 2018 sets out six key principles which are your main responsibilities when processing personal information for the law enforcement purposes. The principles are broadly the same as those in the UK GDPR and are compatible.

The rights of individuals

You should always check your local data protection policies and procedures or contact your Data Protection lead if an individual has asked you to delete their data.

The UK GDPR gives individuals specific rights over their personal data (or information). In summary an individual's rights are:

- the right to access personal data held about them (the right of subject access)
- the right to be informed about how and why their data is used – a Privacy Notice details privacy information
- the right to have data rectified, erased or restricted
- the right to object
- the right to portability of data; and
- the right not to be subject to a decision based solely on automated processing

Further information can be found on the ICO's website³¹ and you should seek legal advice when these rights may or may not apply to your particular case.

³¹ [A guide to individual rights | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

Data protection definitions

Consent	<p>Consent is one of the lawful bases for processing personal information under Article 6 and article 9 of the UK GDPR. Consent is not generally the most appropriate lawful basis to rely on when sharing information for safeguarding or child welfare purposes.</p> <p>The UK GDPR sets a high standard for consent. It must be specific, freely given, unambiguous, time limited and capable of being withdrawn. The data subject (the individual to whom the personal information relates) must have given consent freely and without conditions attached to the processing of their personal information for one or more specific purposes. The individual must also be allowed to freely withdraw their consent at any time and the processing of that data must stop.</p>
Data Protection Impact Assessment (DPIA)	<p>A DPIA³² is a risk assessment process designed to help you analyse, identify and minimise data protection risks of a project or plan. It is a key part of your accountability obligations under the UK GDPR and demonstrates how you comply with all of your data protection obligations.</p> <p>Whilst DPIAs are only mandatory where there is high risk to individuals, as is the case with children due to their vulnerability, they are a useful tool when planning a data share, to help users justify their reason and to establish a lawful basis for sharing. You should carry out a DPIA to assess and mitigate risks to the rights and freedoms of children.</p> <p>A DPIA must be completed before the processing or sharing commences to adequately assess the risks and mitigate them. DPIAs do not have to be complex or time-consuming in every case, but there must be a level of rigour in proportion to the privacy risks arising.</p> <p>There is no definitive DPIA template³³ that you must follow, which means that you can develop your own template and process to suit your particular needs. However, the ICO website provides a template for you to use. A previous or existing DPIA might also help you to prepare your new DPIA, if it covered a similar processing operation.</p> <p>Seek advice from your organisation's designated safeguarding children professional, the Data Protection or Information Governance leads (e.g., Data Protection Officer), Caldicott Guardian, Professional Regulator (if applicable) or your organisation's relevant policy or legal team for further advice.</p>

³² Data Protection Impact Assessments (DPIAs) | ICO

³³ Example DPIA template can be found on the ICO website at <https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx>

Data Sharing Agreements (DSA)	Data Sharing Agreements (DSA) ³⁴ , also known as Information sharing agreements (ISA), are not mandatory but are good practice and helpful to all parties with whom or which you share information. Drawing up an agreement helps ensure everyone is clear about what information is or will be shared, and how it will be done.
Lawful basis	<p>You must have a valid lawful basis³⁵ in order to process personal data.</p> <p>Article 6 UK GDPR provides six 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, the type of organisation you work for, and your relationship with the individual.</p> <p>Most lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you will not have a lawful basis.</p> <p>You must determine your lawful basis before you begin processing, and you should document it.</p> <p>The ICO has published an interactive guidance tool³⁶ to help you determine the lawful basis on which you need to share data.</p>
Legal Obligation	<p>Legal obligation provides a lawful basis where the processing of information is necessary in order to comply with the law. This will not apply to contractual obligations.</p> <p>This does not mean that there must be a legal obligation 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.</p>
Legitimate Interests	This is a lawful basis for processing personal data, which may be appropriate for organisations in the private and voluntary sectors. Sharing information under this basis is likely to be used in situations where you need to use an individual's personal data in ways people would reasonably expect and which are low-risk and will not have a big impact on them.
Personal Data (or personal information)	Personal data ³⁷ (or personal information) is information that relates to an identified or identifiable living individual. An identifiable individual means a person who can be identified directly or indirectly in particular by reference to:

³⁴ [Data sharing agreements | ICO](#)

³⁵ [Lawful basis for processing | ICO](#)

³⁶ [Lawful basis interactive guidance tool | ICO](#)

³⁷ [What is personal data? | ICO](#)

	<p>a) an identifier such as a name, an identification number, location data or an online identifier; or</p> <p>b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.</p>
Practitioner	An individual working with children and young people who makes decisions about sharing personal data on a case-by-case basis. In this guidance, this includes individuals working in any type of organisation or business.
Privacy Notice or Privacy Information	<p>You must provide information to individuals to tell them what is happening to their data and what you plan to do with it. This is information which outlines your purposes for processing someone's personal data, your retention periods for that personal data, and who it will be shared with. However, there are some circumstances in which you don't have to do this. Please see detailed guidance on the ICO website:</p> <p>The Children's Commissioner's Office has published a child friendly privacy policy³⁸ which offers an example.</p>
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data. This includes collecting, storing, recording, consulting, using, amending, analysing, disclosing, restricting or deleting it.
Public Task	This is a lawful basis for processing personal data where a specific task is carried out in the public interest, and which is laid down by law; or the processing is needed in the exercise of official authority (e.g. a public body's tasks, functions, duties or powers) which is laid down by law. You do not need to have a statutory power, so long as there is a clear basis in law.
Special category data	<p>Under the UK GDPR, personal data which is considered sensitive and needs more protection, such as:</p> <ul style="list-style-type: none"> • personal data revealing racial or ethnic origin • personal data revealing political opinions • personal data revealing religious or philosophical beliefs • personal data revealing trade union membership • genetic data • biometric data (where used for identification purposes) • data concerning health • data concerning a person's sex life; and

³⁸ [Your privacy | Children's Commissioner for England \(childrenscommissioner.gov.uk\)](https://www.childrenscommissioner.gov.uk/your-privacy/)

- data concerning a person's **sexual orientation**

In order to share special category data, you need a lawful basis under Article 6 and must also be able to identify a condition for processing under Article 9 of the UK GDPR. Some of the conditions for processing also require you to meet additional conditions, as supplemented by s.10 and Schedule 1 to the Data Protection Act 2018. Safeguarding of children and individuals at risk is one of the substantial public interest conditions under which sharing of special category data may be authorised under Article 9. Guidance to help you is on the ICO website³⁹.

For law enforcement processing under Part 3 of the DPA 2018, the term used is 'sensitive processing' and the provisions are slightly different.⁴⁰

³⁹ [Special category data | ICO](#)

⁴⁰ [Law enforcement processing: Part 3 DPA 2018; and sharing with competent authorities under the GDPR and Part 2 DPA 2018 | ICO](#)

Annex B: Useful resources and advice

- Multi-agency public protection arrangements (MAPPA): Guidance - GOV.UK (www.gov.uk)
- Children missing education - GOV.UK (www.gov.uk)
- The Information Commissioner's Office (ICO) website
- National Police Chief's Council (NPCC) Data sharing- share with confidence guidance 2023
- Safeguarding Data Sharing Agreement Guidance
- Safeguarding Data Sharing Agreement (DSA)
- ICO Data Sharing Hub
- Data sharing code of practice
- ICO Guide to Data Protection
- ICO Guidance: Children and the UK GDPR
- NHSX Information guidance hub - For health and social care professionals
- NHS Digital - Data Security and Information governance hub
- Working Together to Safeguard Children 2023
- Keeping children safe in education
- Eight Caldicott Principles
- The Child Safeguarding Practice Review and Relevant Agency (England) Regulations 2018
- The Non-Maintained Special Schools (England) regulations 2015
- The NHS Confidentiality Code of Practice 2003
- Confidentiality: NHS Code of Practice – Supplementary Guidance on Public interest Disclosures
- Protecting children and young people: The responsibilities of all doctors - ethical guidance summary - GMC (gmc-uk.org)
- Use and share information with confidence - NHS Transformation Directorate (england.nhs.uk)



Department
for Education

© Crown copyright 2024

This publication is licensed under the terms of the Open Government Licence v3.0, except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3.

Where we have identified any third-party copyright information, you will need to obtain permission from the copyright holders concerned.

About this publication:

enquiries <https://www.gov.uk/contact-dfe>
download www.gov.uk/government/publications

Follow us on Twitter: [@educationgovuk](https://twitter.com/educationgovuk)

Connect with us on Facebook: facebook.com/educationgovuk