Department for Education

DRAFT Information sharing advice for practitioners providing safeguarding services to children, young people, parents and carers

June 2023

Contents

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

1. **Protecting a child or young person from harm is more important than protecting their privacy, or the privacy of the person(s) responsible for their care and wellbeing or who might be causing them harm.** The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) provide a framework to support information sharing where practitioners have reason to believe failure to share information may result in the child or young person being at risk of harm.
2. **Wherever it is practicable and safe to do so, engage with the child , young person 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 act in this way if you have reason to believe that doing so may put the child or young person at increased risk of harm (e.g., because their carer(s) may harm the child or young person, react violently, or become less cooperative, or because the child might withhold information or withdraw from services).
3. **You do not need consent to share personal information about a child or young person and/or members of their family if a child or young person is at risk or perceived risk of harm.** You need a lawful basis to share information under data protection law, but consent as a lawful basis is unlikely to be the appropriate one to use when safeguarding or promoting the welfare of a child or young person . However, it continues to be good practice to ensure transparency and to inform the child and carers that you are sharing information and seek to work cooperatively with them wherever possible.
4. **Seek advice promptly whenever you are uncertain or do not fully understand the legal framework that supports information sharing.** Do not leave a child or young person at risk because you have concerns about the possible consequences of sharing information. Find out who in your organisation/agency can provide advice about information sharing or you can consult your professional regulator (if applicable). In your agency/organisation, this may be the designated safeguarding children professional, the data protection/information governance lead (e.g., Data Protection Officer), 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/young person, 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/young person 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 and proportionate for the intended purpose. If you are unsure about the necessity and proportionality of what to share, speak to one of the afore mentioned experts who will be able to assist you.
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

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 and promote their welfare. It should be read alongside the statutory guidance *Working together to safeguard children 2018*[1]). The advice:

1. outlines the responsibilities of agencies/organisations and the golden rules to promote effective information sharing;
2. summarises the key responsibilities of practitioners who share and process personal information and/or have responsibility for deciding how to process it; and
3. explains the lawful bases that may be most appropriate for sharing personal information in a safeguarding context

This 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.

Practitioners should consider this advice alongside guidance relevant for their profession or service area. For example, health practitioners should consider the GMC guidance on *'Confidentiality: Good practice in Handling Patient Information*'[2] and *'Protecting Children and Young People'*[3].

What is this advice for?

The purpose of this advice is to:

- instil confidence in practitioners about the legal framework that supports the sharing of information for safeguarding and promotion of welfare purposes;
- 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;
- support organisations to develop processes, policies and training for their practitioners about information sharing.

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;

[1] Working Together to Safeguard Children 2018 (publishing.service.gov.uk)
[2] Confidentiality: good practice in handling patient information - ethical guidance - GMC (gmc-uk.org)
[3] Protecting children and young people: The responsibilities of all doctors - ethical guidance summary - GMC (gmc-uk.org)

- join up “pieces of the jigsaw” for practitioners, so a true picture of what is happening in a child or young person’s life can be understood;
- assist children, young people and families to receive support from across local agencies/organisations that meets their needs;
- promote joined up working between practitioners and agencies/organisations through a collective understanding about information sharing.

Who is the 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, young people, parents, carers and families, in sectors such as social care, education, health, justice and voluntary.

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

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 and young people.

Senior leaders should create an environment in local safeguarding systems where practitioners feel confident about when and how to share information if a child is at risk or perceived risk of harm.

What do we mean by “safeguarding”?

As defined in Working Together to Safeguard Children 2018, safeguarding and promoting the welfare of children and young people is defined for the purposes of this guidance as follows:

a. protecting children from maltreatment;

b. preventing impairment of children’s mental and physical 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

What do we mean by "harm"?

As defined in section 31 of the Children Act 1989[4], "Harm" means the ill-treatment or the impairment of health or development of a child or young person, including, for example, impairment suffered from seeing or hearing the ill-treatment of another.

What do we mean by "information sharing"?

Information sharing in a safeguarding context means the appropriate and secure exchange of personal information, between agencies and organisations, in order to keep children and young people safe from harm.

Why is information sharing important?

Information sharing is essential for identifying patterns of behaviour, or circumstances, including but not limited to:

- child abuse, neglect or exploitation;
- when a child or young person is at risk of going missing or has gone missing (or a child is missing education);
- when multiple children or young people appear linked to the same risk; or
- where there may be multiple local authorities and agencies/organisations involved in the care of a child or young person's care.

Does data protection legislation 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 and promoting the welfare of 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 or young person.

What is a lawful basis[5]?

Under data protection law, you must have a valid lawful basis (reason) 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 Tool[6] or refer to the definitions in Annex A of this guidance for more help on this.

Which lawful bases are most relevant for safeguarding and promoting the welfare of a child or young person?

There are six lawful bases 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

[4] s.105 and s.31(9) of the Children Act 1989
[5] Lawful basis for processing | ICO
[6] : Lawful basis interactive guidance tool | ICO

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.

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 or young person (e.g. when exercising statutory duties in relation to the safeguarding and promotion of welfare of children found in the Children Acts of 1989 and 2004 and other related legislation). If you work with children, young people 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.

Where the information to be shared is "special category data" it will also be necessary to find a condition for processing the information under Article 9[7] 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. Some Article 9 conditions also need to meet further conditions and safeguards under Schedule 1 of the DPA 2018.

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

Why is consent 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: 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 a safeguarding context, where the overarching consideration will be whether information needs to be shared in order to safeguard and promote the welfare of a child. 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.

[7] Special category data | ICO

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

Why does "consent" cause confusion?

The term "consent" can be used to mean different things in a safeguarding context and these meanings are often conflated and confused. Some meanings of "consent" include:

- **"Consent" as a lawful basis to share information**, as defined by data protection legislation. As already discussed, this is not usually an appropriate legal basis to share personal information in safeguarding contexts. This is the definition of "consent" that is relevant for this guidance.
- "**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. This type of agreement is separate to the permission to share personal information for data protection purposes. 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[8].
- **Being upfront, transparent and honest** with children, young people 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 do I share information and retain a trusted relationship with children, young people and families?

Trusted relationships are at the heart of your work with children, young people and families. It is always good practice to work collaboratively with families and to communicate and listen. This is important and necessary when sharing information about the children and families you are working with. Whenever it is safe and practical to do so, you should engage and explain who you intend to share information with, what information you will be sharing and why.

If you have a duty to share information, and the child or carer therefore does not have a choice, the family should still be informed of this wherever possible. If you are able to offer them a choice about how their information is shared or used, this is preferrable, where it is safe and practical to do so. Being upfront, transparent, and

[8] Consent and confidential patient information - NHS Transformation Directorate (england.nhs.uk)

honest can give young people the confidence to make disclosures and supports parents' willingness to engage with services that provide family support.

Where children, young people and families object to information sharing but you share nonetheless you must record your reasons and the legal basis for doing so.

What is the common law duty of confidentiality?

The duty of confidentiality is one of common law, which means it derives from caselaw, as opposed to statute.

When an individual shares personal information with you in the expectation that this information will be treated confidentially, you will need to consider the duty of confidentiality when deciding whether to share the personal information.

The duty of confidentiality does not necessarily prevent the sharing of information. If sharing without consent, confidential information can be shared on certain grounds:

- where legally required (e.g. because legislation or a court order mandates information sharing); or
- where there is an overriding and specific public interest in disclosure (e.g. where the sharing is necessary for safeguarding purposes) which outweighs the public interest in maintaining confidentiality, and the disclosure is proportionate i.e. no more than necessary.

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

NHS Practitioners:

The first priority for NHS staff is to provide clinical treatment and care, which requires a relationship of trust with patients and their families. Generally, the entire content of a GP or hospital record is subject to the duty of confidentiality. Any decision to share confidential patient information about children, young people and members of their family without consent, with a practitioner outside the care team, must be made in line with the duty of confidentiality. When considering whether there is an overriding public interest that requires the disclosure of patient information, NHS Practitioners will need to take into account the possible impact on the relationship of trust, and whether this might lead to withdrawal from treatment – with its associated safeguarding risks – or undermining of public trust in healthcare services. **These considerations must be balanced with the potential risks of not sharing information and the benefits to the child or young person that will arise from sharing the information.**

According to the GMC guidance on Protecting Children and Young People , 'You must weigh the harm that is likely to arise from not sharing the information against the possible harm, both to the person and to the overall trust between doctors and patients of all ages, arising from releasing that information. If a child or young person with capacity, or a parent, objects to information being disclosed, you should consider their reasons, and weigh the possible consequences of not sharing the information against the harm that sharing the information might cause. If a child or young person is at risk of, or is suffering, abuse or neglect, it will usually be in their best interests to share information with the appropriate agency.'

What is the Human Rights Act 1998?

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 8[9] of the ECHR), can sometimes be seen as a barrier to sharing information. However, where disclosure or sharing of personal information complies with data protection legislation, the sharing or disclosure of that information is also likely to comply with the Human Rights Act.

[9] 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

Who is responsible for sharing information?

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

It is for local safeguarding partners[10] to consider how they will build positive relationships with other local agencies/organisations (which may cross geographical borders) to ensure that relevant information is shared in a timely and proportionate way.

Why is it important to share information with colleagues outside of my organisation?

It is likely that practitioners working in different agencies/organisations that have contact with children or young people 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, young people 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.

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 or young person, it is important to act on those concerns.

The most important consideration is whether the sharing of information is likely to support the safeguarding andprotection of a child or young person.

Should practitioners provide feedback to agencies/organisations about the information they have shared?

When attempting to safeguard a child or young person, practitioners should act in accordance with local procedures and, unless there is a sound reason not to, they should provide feedback[11] on decisions taken, 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.

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

[11] Feedback on referrals to the local authority children's social care is outlined at para 23 of Working Together 2018

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

How do I justify sharing information to safeguard or promote the welfare of a child?

Sharing information for safeguarding purposes can be justified solely based on preventing harm to a child or young person. 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 or promote the welfare of a child or young person. It is only through sharing information that agencies/organisations and practitioners build a richer picture of the day-to-day life of the child, young person 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.

How do I share information, including personal information, with other agencies/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/organisations you are able to share safeguarding information with and what they can do with the information. Seek advice whenever you are uncertain.

Leaders of organisations and agencies with safeguarding responsibilities should ensure robust information sharing arrangements are in place and practitioners are supported to understand local information sharing processes and procedures.

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

Before sharing any personal information as part of a formal and planned sharing exercise, you/your agency/organisation should carry out a Data Protection Impact Assessment (DPIA). It is mandatory to do so in some circumstances, but it is good practice and a helpful process for you to follow even when it is not required by law, as it helps you to assess the risks involved in the planned sharing.

The sharing of personal information must be necessary, fair and proportionate – information must not be shared if it is not relevant. 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/organisation.

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/information governance lead (e.g., Data Protection Officer) to determine the correct route within your agency/organisation.

Any information which you think could have an impact on the welfare of a child/young person should be shared with relevant agencies/organisations.

Who should I contact if I am unsure whether to share information?

Practitioners should use their judgement when making decisions about what information to share, and the agency/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 from your agency/organisation's designated safeguarding children professional, the data protection/information governance lead (e.g., Data Protection Officer), Caldicott Guardian, professional regulator (if applicable) or your organisation's relevant policy or legal team.

What do I tell the people whose information I 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, young person 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 or young person 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.

What should I do if I need to share 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, 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 or young person. 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 Practice[12] which contains guidance on sharing in an urgent situation or in an emergency.

How early should I share information?

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 or young people, whether this is when problems are first emerging (e.g. persistent school absences), or where a child or young person 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).

Sharing and acting on that information early, helps to ensure that a child or young person, 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/organisation may hold the key information in the jigsaw that confirms or corroborates the safeguarding risk.

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 or young person's life.

Practitioners should also be alert to the potential need to share important information about any adults with whom that child or young person has contact, which may impact the child or young person's safety or welfare. 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 so[13]. 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 or young person, 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 or young person suffering harm.

Being alert to signs of abuse and neglect and taking action

All practitioners should be professionally curious and alert to the signs and triggers of abuse and neglect. Children and young people may be vulnerable to neglect, abuse or exploitation from within their family and/or from individuals/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, young person 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;

[12] Data sharing: a code of practice | ICO
[13] See pages 5-8 of this advice for more detail on data protection law.

- neglect (i.e., a child or young person 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/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/alcohol abuse.

Whatever the form of abuse or neglect, practitioners should put the needs of children and young people first when determining what action to take. Standalone guidance for responding to specific abuses and harms, including many of those listed above, is available via gov.uk.[14]

Children and young people 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 or young people 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 or young people of all ages. There will be occasions when children and young people do not realise or recognise that they are being abused or exploited.

Where to report concerns about a child's safety or welfare

If a practitioner has concerns about a child or young person's safety or welfare, even if the practitioner considers it to be a low-level concern they should share the information with local authority children's social care in line with local procedures. Concerns about any child, including children who may already have a social worker, should be shared. Every organisation/agency should have clear guidance on how and when to do this. 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.

[14] Welcome to GOV.UK (www.gov.uk)

Annex A: Data Protection

What is 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/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/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.

Information should only be shared to achieve its relevant purpose.

Data sharing code of practice

The Information Commissioner's Office (ICO) has produced a statutory data sharing code of practice. The code is published on the ICO's data sharing information hub which also contains a range of other data sharing resources. The code is designed to provide practical guidance for organisations in all agencies/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 principles[15] 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, sharing data for law enforcement purposes, you need to consider Part 3 of the Data Protection Act 2018. Part 3, Chapter 2 of the Data 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.

[15] The principles | ICO

The rights of individuals [16]

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 website and you should seek legal advice when these rights may or may not apply to your particular case.

Data protection definitions

Consent	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. 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.
Data Protection Impact Assessment (DPIA)	A DPIA[17] 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. 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

[16] Individual rights | ICO

[17] Data Protection Impact Assessments (DPIAs) | ICO

	should carry out a DPIA to assess and mitigate risks to the rights and freedoms of children. 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. There is no definitive DPIA template[18] 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. Seek advice from your organisation's designated safeguarding children professional, the Data Protection/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.
Data Sharing Agreements (DSA)	Data Sharing Agreements (DSA)[19], also known as Information sharing agreements (ISA), are not mandatory but are good practice and helpful to all parties with whom /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[20]	You must have a valid lawful basis in order to process personal data. 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. 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. You must determine your lawful basis before you begin processing, and you should document it.

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

[19] Data sharing agreements | ICO

[20] Lawful basis for processing | ICO

	The ICO has published an interactive guidance tool to help you determine the lawful basis on which you need to share data, which can be found at Lawful basis interactive guidance tool | ICO.
Legal Obligation	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. 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.
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 [21](or personal information)	Personal data (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: a) an identifier such as a name, an identification number, location data or an online identifier; or b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
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 / Privacy Information	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:

[21] What is personal data? | ICO

	The Children's Commissioner's Office has published a child friendly privacy policy which offers an example: Your privacy | Children's Commissioner for England (childrenscommissioner.gov.uk)
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	Under the UK GDPR, personal data which is considered sensitive and needs more protection, such as: • 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 • 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 website[22]. For law enforcement processing under Part 3 of the DPA 2018, the term used is 'sensitive processing' and the provisions are slightly different.[23]

[22] Special category data | ICO

[23] 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 2018
- Keeping children safe in education
- 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 2003
- Confidentiality: NHS Code of Practice – Supplementary Guidance on Public interest Disclosures
- General Medical Council (GMC) guidance: 'Protecting Children and Young People: The responsibilities of all doctors'

Department for Education

About this publication:

enquiries www.education.gov.uk/contactus
download www.gov.uk/government/publications

Follow us on Twitter: @educationgovuk

Like us on Facebook: facebook.com/educationgovuk