



HM Government

Information sharing

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

July 2018

Contents

Summary	3
About this government advice	3
The seven golden rules to sharing information	4
Sharing Information	6
Being alert to signs of abuse and neglect and taking action	6
Legislative framework	7
The principles	9
Necessary and proportionate	9
Relevant	9
Adequate	9
Accurate	9
Timely	9
Secure	10
Record	10
When and how to share information	11
When	11
How	11
Flowchart of when and how to share information	12
Myth-busting guide	13
Useful resources and external organisations	15
Other relevant departmental advice and statutory guidance	15

Summary

Information sharing is essential for effective safeguarding and promoting the welfare of children and young people. It is a key factor identified in many serious case reviews (SCRs), where poor information sharing has resulted in missed opportunities to take action that keeps children and young people safe.

About this government advice

This HM Government advice is non-statutory, and has been produced to support practitioners in the decisions they take to share information, which reduces the risk of harm to children and young people and promotes their well-being.

This guidance does not deal in detail with arrangements for bulk or pre-agreed sharing of personal information between IT systems or organisations other than to explain their role in effective information governance.

This guidance has been updated to reflect the General Data Protection Regulation (GDPR) and Data Protection Act 2018, and it supersedes the HM Government *Information sharing: guidance for practitioners and managers* published in March 2015.

Who is this advice for?

This advice is for all frontline practitioners and senior managers working with children, young people, parents and carers who have to make decisions about sharing personal information on a case-by-case basis. It might also be helpful for practitioners working with adults who are responsible for children who may be in need.

The seven golden rules to sharing information

1. Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.
5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

The General Data Protection Regulation (GDPR) and Data Protection Act 2018

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 introduce new elements to the data protection regime, superseding the Data Protection Act 1998. Practitioners must have due regard to the relevant data protection principles which allow them to share personal information,

The GDPR and Data Protection Act 2018 place greater significance on organisations being transparent and accountable in relation to their use of data. All organisations handling personal data need to have comprehensive and proportionate arrangements for collecting, storing, and sharing information.

The GDPR and Data Protection Act 2018 do not prevent, or limit, the sharing of information for the purposes of keeping children and young people safe.

To effectively share information:

- all practitioners should be confident of the processing conditions, which allow them to store, and share, the information that they need to carry out their safeguarding role. Information which is relevant to safeguarding will often be data which is considered 'special category personal data' meaning it is sensitive and personal
- where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information **without consent**
- information **can be shared legally without consent**, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place a child at risk.
- relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being.

Sharing Information

Sharing information is an intrinsic part of any frontline practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. Information sharing helps to ensure that an individual receives the right services at the right time and prevents a need from becoming more acute and difficult to meet.

Poor or non-existent information sharing is a factor repeatedly identified as an issue in Serious Case Reviews (SCRs) carried out following the death of or serious injury to, a child. In some situations, sharing information can be the difference between life and death.

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. Every practitioner must take responsibility for sharing the information they hold, and cannot assume that someone else will pass on information, which may be critical to keeping a child safe.

Professor Munro's review of child protection concluded the need to move towards a child protection system with less central prescription and interference, where we place greater trust in, and responsibility on, skilled practitioners at the frontline.¹ Those skilled practitioners are in the best position to use their professional judgement about when to share information with colleagues working within the same organisation, as well as with those working within other organisations, in order to provide effective early help, to promote their welfare, and to keep children safe from harm.

Lord Laming emphasised that the safety and welfare of children is of paramount importance and highlighted the importance of practitioners feeling confident about when and how information can be legally shared.² He recommended that all staff in every service, from frontline practitioners to managers in statutory services and the voluntary sector should understand the circumstances in which they may lawfully share information, and that it is in the public interest to prioritise the safety and welfare of children.

Being alert to signs of abuse and neglect and taking action

All practitioners should be alert to the signs and triggers of child abuse and neglect.³ Abuse (emotional, physical and sexual) and neglect can present in many different forms. Indicators of abuse and neglect may be difficult to spot. Children may disclose abuse, in

¹ [The Munro review of child protection: final report – a child centred system](#)

² [The Protection of Children in England: a progress plan](#)

³ [What to do if you're worried a child is being abused](#)

which case the decision to share information is clear, as actions must be taken to respond to the disclosure. In other cases, for example, neglect, the indicators may be more subtle and appear over time. In these cases, decisions about what information to share, and when, will be more difficult to judge. Everyone should be aware of the potential for children to be sexually exploited for money, power, or status, and individuals should adopt an open and inquiring mind to what could be underlying reasons for behaviour changes in children of all ages.

If a practitioner has concerns about a child's safety or welfare, they should share the information with the local authority children's social care, NSPCC and/or the police, in line with local procedures. Security of information sharing must always be considered and should be proportionate to the sensitivity of the information and the circumstances. If it is thought that a crime has been committed and/or a child is at immediate risk, the police should be notified immediately.

Legislative framework

Key organisations who have a duty under section 11 of the Children Act 2004 to have arrangements in place to safeguard and promote the welfare of children are:

- the local authority;
- NHS England;
- clinical commissioning groups;
- NHS Trusts, NHS Foundation Trusts;
- the local policing body;
- British Transport Police Authority;
- prisons;
- National Probation Service and Community Rehabilitation Companies;⁴
- youth offending teams; and
- bodies within the education and /or voluntary sectors, and any individual to the extent that they are providing services in pursuance of section 74 of the Education and Skills Act 2008.

⁴ The duty under section 11 of the Children Act 2004 will apply to Community Rehabilitation Companies via contractual arrangements entered into by these bodies with the Secretary of State under Section 3 of the Offender Management Act 2007.

There are also a number of other similar duties, which apply to other organisations. For example, section 175 of the Education Act 2002 which applies to local authority education functions and to governing bodies of maintained schools and further education institutions, and section 55 of the Borders, Citizenship and Immigration Act 2009 which applies to the immigration, asylum, nationality and customs functions of the Secretary of State (in practice discharged by UK Visas and Immigration, Immigration Enforcement and the Border Force, which are part of the Home Office).

Where there are concerns about the safety of a child, the sharing of information in a timely and effective manner between organisations can improve decision-making so that actions taken are in the best interests of the child. The GDPR and Data Protection Act 2018 place duties on organisations and individuals to process personal information fairly and lawfully; they are not a barrier to sharing information, where the failure to do so would cause the safety or well-being of a child to be compromised. Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns.

All organisations should have arrangements in place, which set out clearly the processes and the principles for sharing information internally. In addition, these arrangements should cover sharing information with other organisations and practitioners, including third party providers to which local authorities have chosen to delegate children's social care functions, and any Local Safeguarding Children Board (LSCB) still operating within the local authority area as well as safeguarding partners (please see below).

One approach to aid effective information sharing is the use of Multi-Agency Safeguarding Hubs, where teams may be co-located physically or locally. In these settings, it is important that accountability is defined to ensure that teams know who is responsible for making decisions and that actions taken are in the best interest of the child.

Safeguarding partners (as defined in Section 16E of the Children Act 2004) and LSCBs (where still in operation) should play a strong role in supporting information sharing between and within organisations and addressing any barriers to information sharing. This should include ensuring that a culture of appropriate information sharing is developed and supported as necessary by multi-agency training.

Safeguarding partners and LSCBs (where still in operation) can require a person or body to comply with a request for information, as outlined in sections 16H and 14B of the Children Act 2004, respectively. This can only take place when the information requested is for the purpose of enabling or assisting the safeguarding partners or LSCB to perform their functions. Any request for information to a person or body, should be necessary and proportionate to the reason for the request. Safeguarding partners and LSCBs should be mindful of the burden of requests and should explain why the information is needed.

The principles

The principles set out below are intended to help practitioners working with children, young people, parents and carers share information between organisations. Practitioners should use their judgement when making decisions about what information to share, and should follow organisation procedures or consult with their manager if in doubt.

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

Necessary and proportionate

When taking decisions about what information to share, you should consider how much information you need to release. Not sharing more data than is necessary to be of use is a key element of the GDPR and Data Protection Act 2018, and you should consider the impact of disclosing information on the information subject and any third parties. Information must be proportionate to the need and level of risk.

Relevant

Only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make informed decisions.

Adequate

Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

Accurate

Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

Timely

Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection to a child. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore place a child or young person at increased risk of harm. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

Secure

Wherever possible, information should be shared in an appropriate, secure way. Practitioners must always follow their organisation's policy on security for handling personal information.

Record

Information sharing decisions should be recorded, whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with each organisation's own retention policy, the information should not be kept any longer than is necessary. In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so.

When and how to share information

When asked to share information, you should consider the following questions to help you decide if, and when, to share. If the decision is taken to share, you should consider how best to effectively share the information. A flowchart follows the text.

When

Is there a clear and legitimate purpose for sharing information?

- Yes – see next question
- No – do not share

Do you have consent to share?

- Yes – you can share but should consider how
- No – see next question

Does the information enable an individual to be identified?

- Yes – see next question
- No – you can share but should consider how

Have you identified a lawful reason to share information without consent?

- Yes – you can share but should consider how
- No – do not share

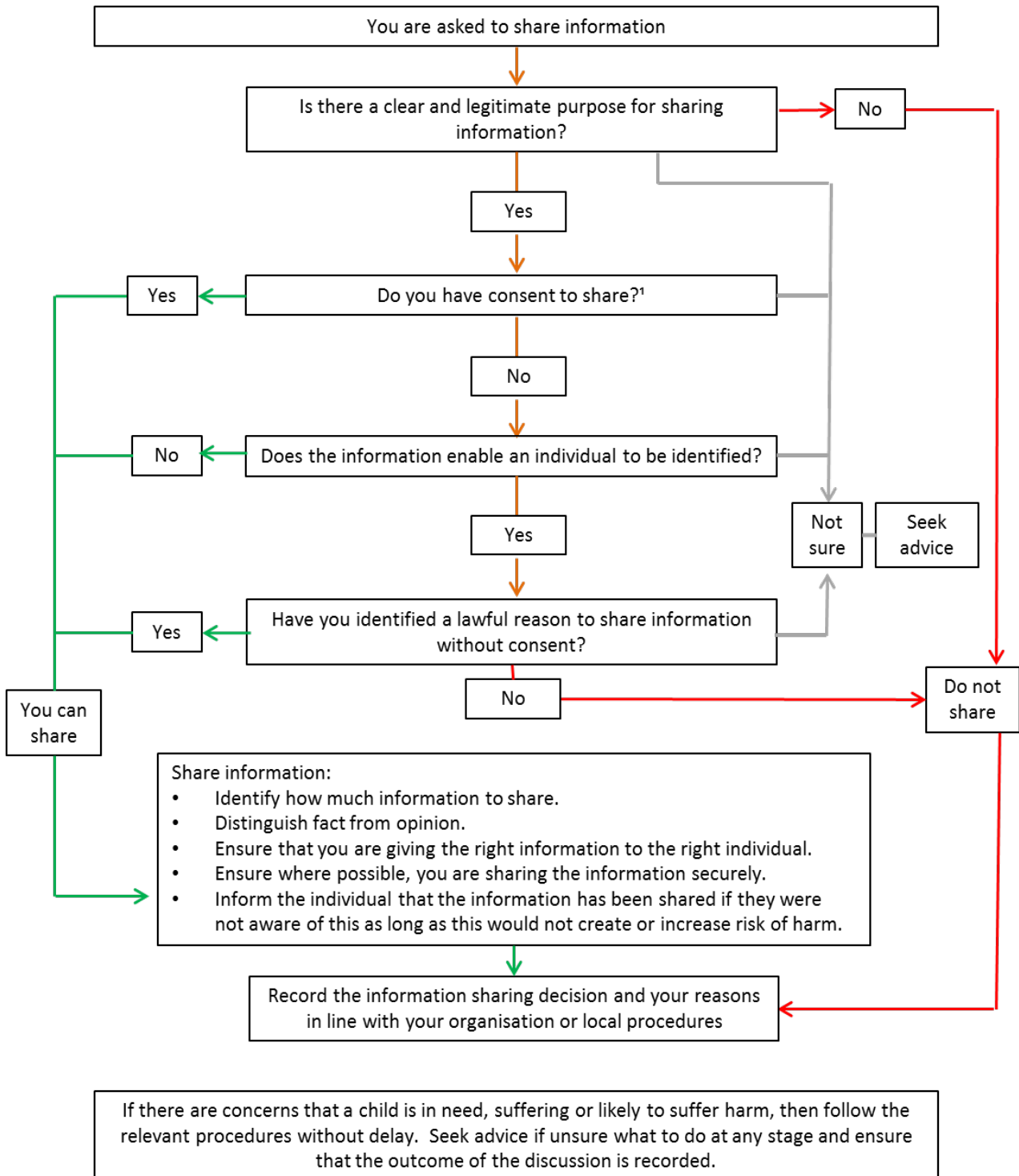
How

- Identify how much information to share
- Distinguish fact from opinion
- Ensure that you are giving the right information to the right individual
- Ensure where possible that you are sharing the information securely
- Where possible, be transparent with the individual, informing them that the information has been shared, as long as doing so does not create or increase the risk of harm to the individual.

All information sharing decisions and reasons must be recorded in line with your organisation or local procedures. If at any stage you are unsure about how or when to

share information, you should seek advice on this. You should also ensure that the outcome of the discussion is recorded.

Flowchart of when and how to share information



1. Consent must be unambiguous, freely given and may be withdrawn at any time

Myth-busting guide

Sharing of information between practitioners and organisations is essential for effective identification, assessment, risk management and service provision. Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children and young people at risk of abuse or neglect. Below are common myths that can act as a barrier to sharing information effectively:

The GDPR and Data Protection Act 2018 are barriers to sharing information

No – the GDPR and Data Protection Act 2018 do not prohibit the collection and sharing of personal information. They provide a framework to ensure that personal information is shared appropriately. In particular, the Data Protection Act 2018 balances the rights of the information subject (the individual whom the information is about) and the possible need to share information about them. Never assume sharing is prohibited – it is essential to consider this balance in every case. You should always keep a record of what you have shared.

Consent is always needed to share personal information

No – you do not necessarily need the consent of the information subject to share their personal information.

Wherever possible, you should seek consent and be open and honest with the individual from the outset as to why, what, how and with whom, their information will be shared. You should seek consent where an individual may not expect their information to be passed on. When you gain consent to share information, it must be explicit, and freely given.

There may be some circumstances where it is not appropriate to seek consent, either because the individual cannot give consent, it is not reasonable to obtain consent, or because to gain consent would put a child or young person's safety or well-being at risk.

Where a decision to share information without consent is made, a record of what has been shared should be kept.

Personal information collected by one organisation cannot be disclosed to another organisation

No - this is not the case, unless the information is to be used for a purpose incompatible with the purpose it was originally collected for. In the case of children in need, or children at risk of significant harm, it is difficult to foresee circumstances where information law would be a barrier to sharing personal information with other practitioners.

Practitioners looking to share information should consider which processing condition in the Data Protection Act 2018 is most appropriate for use in the particular circumstances of the case. This may be the safeguarding processing condition or another relevant provision.

The common law duty of confidence and the Human Rights Act 1998 prevent the sharing of personal information

No - this is not the case. In addition to the GDPR and Data Protection Act 2018, practitioners need to balance the common law duty of confidence, and the rights within the Human Rights Act 1998, against the effect on children or individuals at risk, if they do not share the information.

If information collection and sharing is to take place with the consent of the individuals involved, providing they are clearly informed about the purpose of the sharing, there should be no breach of confidentiality or breach of the Human Rights Act 1998. If the information is confidential, and the consent of the information subject is not gained, then practitioners need to decide whether there are grounds to share the information without consent. This can be because it is overwhelmingly in the information subject's interests for this information to be disclosed. It is also possible that a public interest would justify disclosure of the information (or that sharing is required by a court order, other legal obligation or statutory exemption).

In the context of safeguarding a child or young person, where the child's welfare is paramount, it is possible that the common law duty of confidence can be overcome. Practitioners must consider this on a case-by-case basis. As is the case for all information processing, initial thought needs to be given as to whether the objective can be achieved by limiting the amount of information shared – does all of the personal information need to be shared to achieve the objective?

IT Systems are often a barrier to effective information sharing

No – IT systems, such as the Child Protection Information Sharing project (CP-IS), can be useful in supporting information sharing. IT systems are most valuable when practitioners use the data that has been shared to make more informed decisions about how to support and safeguard a child. Evidence from the Munro Review is clear that IT systems will not be fully effective unless individuals from organisations co-operate around meeting the needs of the individual child. Professional judgment is the most essential aspect of multi-agency work, which could be put at risk if organisations rely too heavily on IT systems.

Useful resources and external organisations

- [The Information Commissioner's Office \(ICO\) website](#)
- [Practice guidance on sharing adult safeguarding information](#)

Other relevant departmental advice and statutory guidance

- [Working Together to Safeguard Children \(2018\)](#)
- [Keeping Children Safe in Education \(2016\)](#)
- [What to do if you're worried a child is being abused \(2015\)](#)



HM Government

© Crown copyright 2018

This publication (not including logos) is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

To view this licence:

visit www.nationalarchives.gov.uk/doc/open-government-licence/version/3

email psi@nationalarchives.gsi.gov.uk

write to Information Policy Team, The National Archives, Kew, London, TW9 4DU

About this publication:

enquiries www.education.gov.uk/contactus

download www.gov.uk/government/publications

Reference: DFE-00128-2018



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



Like us on Facebook:
facebook.com/educationgovuk