

TSAB Guide:

Collaborative Working and Information
Sharing between Professionals to Protect
Adults.

Key Principles:

This guide is aimed at supporting staff who may be required to make case-by-case decisions about sharing information, by offering clarity on when and how information can be shared legally and professionally, in order to achieve improved outcomes for adults at risk of abuse and/or neglect.

- Sharing of information between practitioners and organisations is essential for effective risk identification, assessment and management, and service provision. Fears about sharing information should not stand in the way of the need to safeguard and promote the welfare of adults at risk of abuse or neglect.
- Adults have a general right to independence, choice and self-determination including control over information about themselves. In the context of adult safeguarding these rights can be overridden in certain circumstances”.
- 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.
- Seek advice from other practitioners, your own organisations policies and procedures and/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.
- Under the UK 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.
- 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.
- 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.
- 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.

Is it necessary or proportionate?

When taking decisions about what information to share, you should consider if the information is:

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

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

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.

Minimised: Information shared should be the minimal amount to achieve the purpose required. In some circumstances, this may mean the sharing of anonymised or pseudonymised data to assist with initial decision making.

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.

Timely: Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection to an adult. 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 an adult at increased risk of harm.

Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

Recorded: 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.

Legislation

A range of legislation and guidance underpins information sharing:

- The Care Act 2014

- Care and Support Statutory Guidance
- Data Protection Act 2018 (DPA 2018)
- UK General Data Protection Regulations (UK GDPR)
- Information Commissioner's Office (ICO) Data Sharing Code of Practice
- The Human Rights Act 1998
- The Common Law Duty of Confidence
- Crime and Disorder Act 1998
- Criminal Justice Act 2003
- Mental Capacity Act 2005
- Mental Capacity (Amendment) Act 2019
- Criminal Procedures and Investigations Act 1996

Other wider legislation includes:

- Crime and Disorder Act 1998
- Freedom of Information Act 2000
- Police and Justice Act 2006
- Safeguarding Vulnerable Groups Act 2006
- The Equality Act 2010
- Protection of Freedoms Act 2012
- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- The Health and Social Care Act 2008 (Regulated Activities) (Amendment) Regulations 2015
- Counter-Terrorism and Security Act 2015 (Section 26 – Prevent Duty)
- Modern Slavery Act 2015
- Mental Health Act 1983
- Mental Health Act 2007
- Common Law Duty of Care.

Information sharing and the Care Act:

- Sections 6 and 7 of the Care Act 2014 set out when local authorities and relevant partners must work cooperatively with each other; when local authorities must cooperate with other appropriate people or bodies; and that local authority officers from different services in the same authority must work cooperatively.
- Section 45 of the Care Act 2014 outlines that Safeguarding Adults Boards in exercising their functions can request a person to supply information to it, or some other person specified in the request, the

person to whom the request is made must comply with the request if particular conditions are met. For example, when requesting information for Safeguarding Adult Reviews, or multi-agency audit.

Duty of Candour:

This means operating with openness and transparency and apologising for harm caused regardless of fault. It applies to all providers regulated by the Care Quality Commission (CQC). When reports are made by staff, people accessing services or the public that relate to this duty, CQC will refer to their safeguarding and whistleblowing protocols where relevant and appropriate.

Common law duties:

Common law duty of care: A common law duty of care to protect the public exists for the Police who may share personal data where it is necessary to prevent harm.

Common law duty of confidence: When anyone wishing to disclose information that is not in a public domain but obtained where it gives rise to a duty of confidence. It will need to be established whether there is an overriding justification for disclosing that information. If not, it is necessary to obtain the informed consent of the person who supplied the information. This will need to be assessed on a case-by-case basis and legal advice should be sought in any case of doubt.

What and when to share:

You can share information for the purpose of safeguarding without consent under the 'safeguarding individuals at risk exemption' in the Data Protection Act 2018 Schedule 8 section 4. The exemption applies to children, and to adults aged 18 and over experiencing or at risk of abuse and neglect, who have needs for care and support, and who cannot protect themselves. This is when the safeguarding duty applies in the Care Act 2014.

This includes all organisations including housing providers and charities.

In safeguarding, the ability to share information without consent, in the public interest, centres on two factors:

- Whether there is evidence or reasonable cause to believe that someone is experiencing, or is at risk of experiencing, neglect, or physical, mental, or emotional harm

And / or

- To prevent harm to someone, including through the prevention,

detection, and prosecution of serious crime.

And it is necessary for one of these reasons:

- In the circumstances, consent to the processing cannot be given by the person;
- In the circumstances, consent cannot reasonably be expected to be obtained;
- Obtaining the consent of the person would prejudice providing protection.

DPA Schedule 8 section 4

Sharing information without consent in safeguarding

If a person refuses intervention to support them with a safeguarding concern, or requests that information about them is not shared with other safeguarding partners, their wishes should be respected. However, there are a number of circumstances where the practitioner can reasonably override such a decision, including:

- the person lacks the mental capacity to make that decision – this must be properly explored and recorded in line with the Mental Capacity Act
- other people are, or may be, at risk, including children
- sharing the information could prevent a crime
- the alleged abuser has care and support needs and may also be at risk
- a serious crime has been committed
- staff are implicated
- the person has the mental capacity to make that decision but they may be under duress or being coerced
- the risk is unreasonably high and meets the criteria for a multi-agency risk assessment conference referral (Marac)
- a court order or other legal authority has requested the information.

Further guidance from the Information Commissioner's Office (ICO) can be found here - [Data sharing: a code of practice | ICO](#).

The purpose of sharing concerns is:

- protecting an individual from neglect or physical, mental, or emotional harm, or
- protecting the physical, mental, or emotional well-being of an individual.

Your lawful basis to share information will, as appropriate, be one of:

- Vital interest: necessary to protect someone's life, emergency treatment.
- Public task: necessary in public interest or for your lawful public function.
- Legitimate interest: necessary to protect someone's legitimate interests [e.g. for a non-public body to protect an individual from abuse and neglect].

Practitioners have highlighted that sharing information without consent may damage their working relationship with the individual. However, the risks of not sharing information should be carefully considered in these situations, including through professional challenge, and decision making should be clearly recorded regardless of the decision taken.

Information sharing with family members:

There may be times when information sharing with family members is appropriate and key to safeguard the adult from harm. The principles within this guide should be applied to sharing information with family members.

Constructive professional challenge:

Collaborative working often involves good inter-agency work and timely information sharing. Where professionals, practitioners, or volunteers have a concern about a decision made by another organisation / team, that concern should be followed up with robust professional challenge.

Professional challenge is a sign of good professional practice and responsibility. All agencies and services should promote a culture which encourages constructive challenge within and between organisations, welcomes different professional perspectives, and acknowledges the important role that challenge can play in safeguarding adults.

[Professional Challenge Procedure | Teeswide Safeguarding Adults Board](#)

Myth-busting

Sharing of information between practitioners and organisations is essential for effective risk identification and assessment. Below are common myths that can act as a barrier to sharing information

effectively.

1. Consent is always needed to share personal information

No – you do not always need consent to share personal information.

Sharing for the purpose of safeguarding adults is different to, for example, seeking consent to provide a service.

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

No – UK 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.

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.

You should always keep a record of what you have shared or not shared and the reasons for either.

3. Personal information collected by one organisation cannot be disclosed to another organisation for safeguarding purposes

No - this is not the case

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.

4. 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 UK 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, individuals at risk, or others, 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 it must be in the subject's interests, or someone else's interests, for this information to be disclosed. For the purpose of safeguarding it is more likely that the public interest test would justify disclosure of the information (or that sharing is required by a court order or other legal obligation, otherwise practitioners need to decide whether there are grounds to share the information without consent. This can be because it is overwhelmingly in the DPA information sharing statutory exemption). If you have any queries contact your organisation's relevant officer.

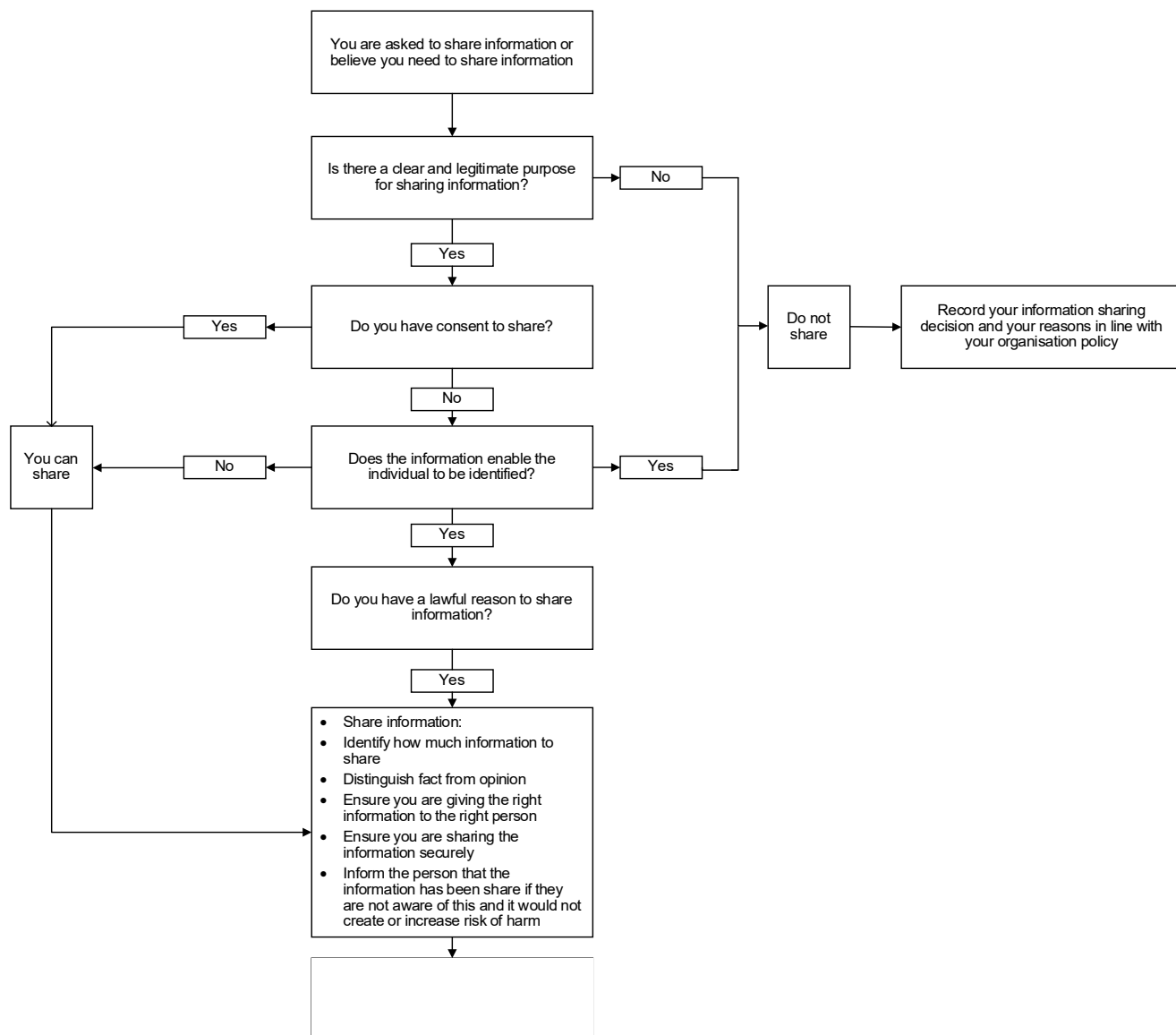
Stop and Consider:

- Have you checked the recommended processes in your organisation's guidance and this document?
- Have you used a level of security appropriate to the information you're about to share?
- Have you asked your line manager or your organisation's Data Protection Officer?

Remember that the UK General Data Protection Regulation (GDPR), Data Protection Act 2018, Data Sharing Code of Practice and The Human Rights Act are not barriers to justified information sharing but provide a framework to ensure that personal information about living individuals is shared appropriately.

Adoption of professional curiosity can help to prevent risk. If there are concerns that a child or an adult may be at risk of serious harm, then it is your duty to follow the relevant procedures without delay.

Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded



Practice points:

It is likely vital interest, public function or legitimate interest will apply as your lawful basis for sharing in most cases for safeguarding, rather than consent (if you cannot offer a genuine choice, consent is not appropriate). Public authorities, employers, and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given."

If you are not sure **seek advice**