Somerset Safeguarding Adults Board
Information Sharing Agreement

Parties

All member organisations of the Somerset Safeguarding Adults Board (SSAB).

Purpose

To support the functions of the Safeguarding Adults Board.

This document

This document explains the need to share information to support the functions of the Safeguarding Adults Board in Somerset.

The Agreement is intended to provide a consistent approach to information sharing across the partnership. It has been produced to support Board represented organisations in the decisions they take when sharing information to support the SSAB's functions.

Sharing the right information, at the right time, with the right people, is fundamental to good practice in safeguarding adults. Fears about sharing information cannot be allowed to stand in the way of the need to protect and meet the needs of vulnerable people.

Introduction to the SSAB

Under the Care Act 2014 a local authority must:

- Set up a safeguarding board; the board will share strategic information to improve local safeguarding practice
- Cooperate with each of its relevant partners; each relevant partner must also cooperate with the local authority.

Clause 45 of the Care Act focuses on 'supply of information'. This relates to the responsibilities of others to comply with requests for information from the Safeguarding Adults Board for the purpose of enabling or assisting it to exercise its functions.

Why do we need to share adult safeguarding information?

Organisations need to share safeguarding information with the right people at the right time to:

- Prevent death or serious harm
- Coordinate effective and efficient responses
- Enable early interventions to prevent the escalation of risk
- Prevent abuse and harm that may increase the need for care and support
- Maintain and improve good practice in safeguarding adults
- Reveal patterns of abuse that were previously undetected and could identify others at risk of abuse
- Identify low level concerns that may reveal people at risk of abuse
- Help people to access the right kind of support to reduce risk and promote wellbeing
- Help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour
- Reduce organisational risk and protect reputation.

The seven golden rules to information sharing

1. **Remember that the General Data Protection Regulation (GDPR) 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. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing *so (you may need to take advice from your data protection officer)*.
3. **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 and, even when sharing without consent, **tell them when information is being shared** unless it is unsafe or inappropriate to do so.
4. Share with consent only where appropriate **and where sharing the information does not fall under a different lawful reason**. Where you have consent, be mindful that an individual would have the expectation that only relevant information would be shared and must have the option to withdraw their consent.
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, is shared securely, and that is arrangements in place for it to be returned or destroyed.
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.

Information to be shared

This agreement does not specify what information should be shared for the Purpose because every decision to share information should be made on a case by case basis. Information that is deemed necessary, relevant and proportionate in one case may not be so in another. Each case is likely to be different.

When and how to share information involves a decision-making process which is set out in the following section.

When and how to share information

When asked or deciding 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 is attached to this Agreement (Appendix 1).

When to share:

Q1 **Is there a clear and legitimate Purpose for sharing information (i.e. is it necessary)?**
- Yes – see next question
- No – do not share

Q2 **Does the information enable an individual to be identified** – *or could it be combined with other available information to enable an individual to be identified*?
- Yes – see next question
- No – you can share but should consider how

Q3 Is the information 'Personal data'[1] or 'Sensitive personal data'[2]?

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

Q4 Is there a lawful basis to share information such as to perform a Public Task or to protect the Vital Interests of the information subject?

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

Q5 Do you need consent? If the information is being shared to ensure safeguarding, for statutory purposes or as part of a public task you do not need consent. Note: the GDPR sets a high standard for consent and this only applies where we are offering individuals real choice and control. In most cases you must still inform the individual that the information has been shared, as long as this would not create or increase any risk of harm

- Yes (*you do need consent to share*) – Ensure that the individual has real choice and control over the information that is to be shared
- No (*you have a lawful basis to share and do not need consent*) – you can share but should consider how, including how you inform the individual

In all circumstances you must record your information sharing decision and you reasons in line with your organisations procedures

How to share:

- 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
- **Inform the individual that the information has been shared, if they were not aware of this, as long as this would not create or increase risk of harm**

In all cases:

- 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 and ensure that the outcome of the discussion is recorded.
- If there are concerns that a child or vulnerable person is suffering or likely to suffer harm, then follow the relevant procedures without delay.

Legal gateway to share

Each party will have a different statutory basis for holding and processing information it needs to fulfil its legal duties. The following are examples of legal gateways that may typically apply and includes those applicable across children's and adults' services:

- Written Consent
- The Children Act 2004 s10
- The Children Act 2004 s11he Children Act 1989 S47
- The Children Act 1989 s27
- Localism Act 2013 s1
- Local Government Act 1972 s111

[1] The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. Source: Information Commissioner's Office

[2] The GDPR refers to sensitive personal data as "special categories of personal data". The special categories specifically include genetic data and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing. Source: Information Commissioner's Office

- Welfare Reform Act 2012 s131
- Care Act 2014
- Mental Capacity Act 2005
- Common law
- Data Protection Act 1998
- Crime and Disorder Act 1998
- Criminal Justice Act 2003

Information sharing mechanism

Information must only be shared/transmitted by secure means, kept secure, access to it limited to those that need to know, and disposed of securely. A privacy notice (see Appendix 2 for suggested template) must be included on all forms.

Benefits of the intended sharing

By ensuring all members of the SSAB have the ability, confidence and trust to share information, those who have been subject to, or are likely to be subject to, harm can be identified in a timely manner, which will help protect and meet the needs of vulnerable people.

Retention

The general principle to be applied is that the information should only be kept for as long as is necessary for the Purpose, and in accordance with the member organisations' own retention guidance or policy.

Dealing with conflict or complaints

If there is continued reluctance from one partner to share information on a safeguarding concern, the matter should be referred to the Board. The Board can then consider whether the concern warrants a request, under Clause 45 of the Care Act, for the 'supply of information'. The reluctant party would only have grounds for refusal if it would be 'incompatible with their own duties or have an adverse effect on the exercise of their functions'. In the event of a complaint relating to the disclosure of the use of individuals personal information that has been supplied under this Agreement, all parties will provide cooperation and assistance to resolve it.

Review date

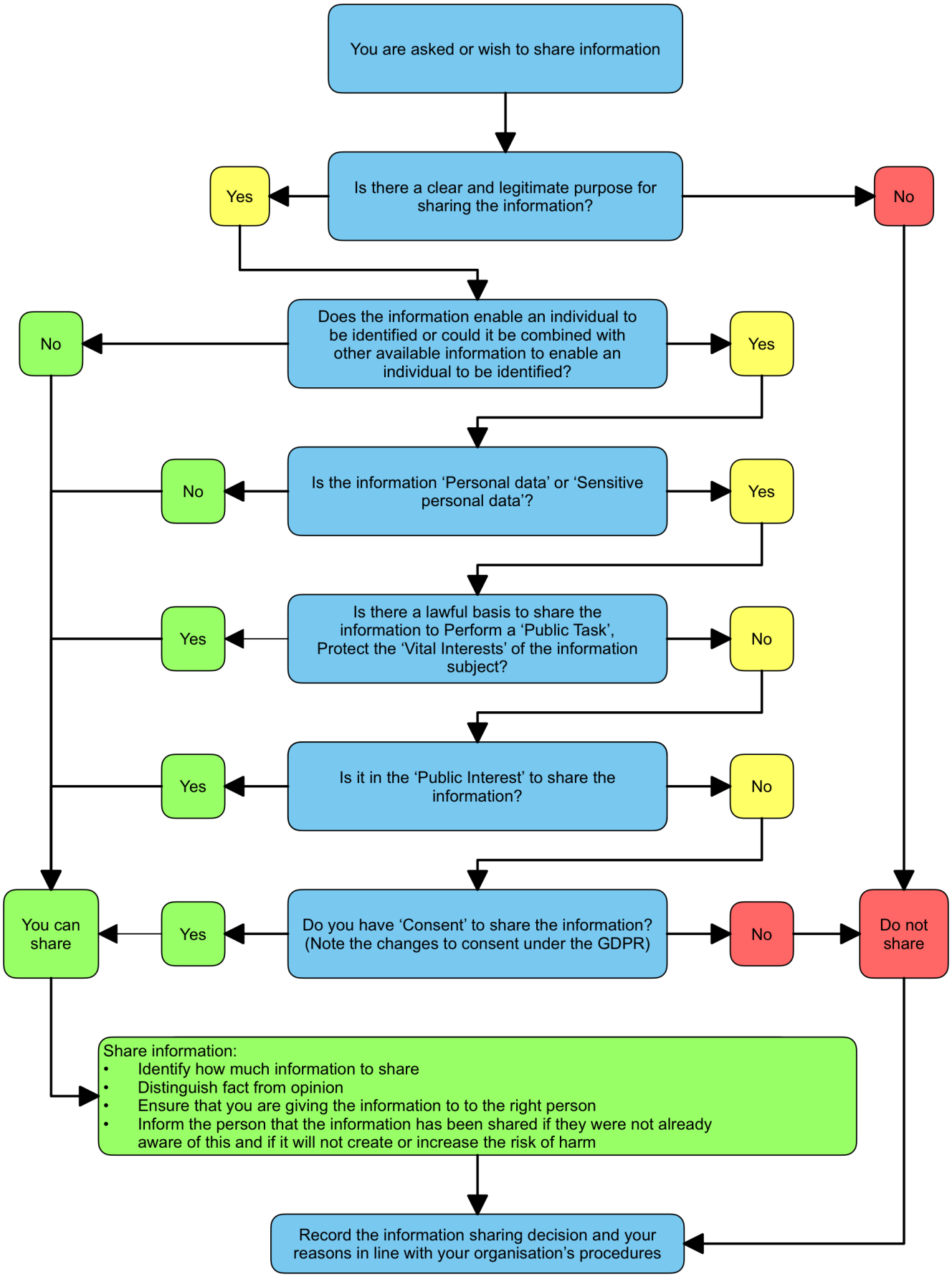
This agreement will be reviewed annually from date of sign off to establish if the sharing remains necessary, still operates as intended and has, or is, achieving the intended benefits. This will also provide the opportunity to review the effective adherence to this Agreement, though any issues will be raised and addressed as they arise.

Signatories:

By signing this document I accept that the organisation I represent will be bound by any conditions imposed in this document:

Appendix 1

Flow chart of when and how to share information



Appendix 2

Template Privacy notice requirement for forms

This must be completed in consultation with organisational information governance leads

Notification regarding the processing of any personal data supplied on this form

Data Controller – The name of your organisation
Data Protection Officer contact – the email address for contact
Purpose for processing – Insert purpose
Legal basis for processing – Insert basis

> ***By Law –*** *used where statutory instrument allows for processing, the statutory instrument must be named*
> ***Legitimate Interests*** *– Used where legal basis for processing is legitimate interests*

Data Sharing – the personal data provided will be shared with insert the name(s) of the organisations or persons with whom the information will be shared
Transfers abroad – insert an explicit statement as to whether the information supplied will this data will be transferred abroad or not **(you must seek advice from your information lead if it will be)**.
Data Retention – this data will be retained for a period of insert number years to meet insert retention requirement requirements
Your Rights – You have the right to ask insert the name of your organisation to a copy of your data, the right to rectify or erase your personal data, and the right to object to processing. However these rights are only applicable if insert the name of your organisation has no other legal obligation concerning that data. You also have the right to complain to the regulator, https://ico.org.uk/
Consequences: To be used where processing is by law or contract. You need to put what consequences are if we do not receive the information; such as: If you do not supply this information to us, we will not be able to do XXXX
For more information see insert link to your privacy statement

For more information see https://gdpr-info.eu/art-13-gdpr/