

# Wiltshire Safeguarding Adults Board Information Sharing Agreement



## Parties

All member organisations of the Wiltshire Safeguarding Adults Board (WSAB).

## 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 Wiltshire.

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 WSAB's functions.

Sharing the right information, at the right time, with the right people, is fundamental 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 WSAB

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 arrangements are 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 and for what 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’<sup>1</sup> or ‘Sensitive personal data’<sup>2</sup>?**
- Yes – see next question
  - No – you can share but should consider how

---

<sup>1</sup> 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

<sup>2</sup> 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

**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 your 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

**Methods used for sharing:**

Within the Safeguarding Process, information may be transferred in the following ways:

- Verbally, face to face, in meetings or on the telephone.
- In written communications, (for example, forms, minutes, letters, statements or reports)
- Transferred in hard copy through internal or external mail services.
- In written information transferred by secure email, or secure file transfer systems.
- Information accessed in situ, via provision of access to organisational databases or records.

When each of these methods is used it is essential to consider the safest way to record and mark the information and to ensure safe transit and delivery. Information should be appropriately secured in transit and transferred by methods aligned to the best practice specified in the “Protecting Information in Government Report – January 2010”.

1. Verbal conversations and interviews should be recorded in a written statement that is agreed by the information giver. Care must be taken to record and denote information clearly as fact, statement or opinion and to attribute any statement or opinion to the owner. All information should be recorded in such a way that it can be used as evidence in court, should that be required at a later date.

2. Meetings should be recorded in minutes that are agreed by the delegates present.
3. Written communications containing confidential information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation. They should be clearly marked "Private & Confidential – to be opened by the recipient only".
4. When files are transferred on electronic digital media devices, the files should be encrypted to an appropriate standard, with decryption keys / passwords supplied separately.
5. When confidential information is sent by email, it should be sent and received using secure government domain email addresses, to ensure encryption of information in transit. The full list of secure Government email systems are below. They have email addresses ending:
  - .cjsm.net (Criminal and Justice)
  - .gcsx.gov.uk (Local Government/Social Services)
  - .gse.gov.uk (Central Government)
  - .gsi.gov.uk (Central Government including Department of Health)
  - .gsx.gov.uk (Central Government)
  - .hscic.gov.uk (The Health and Social Care Information Centre)
  - .mod.uk (Military)
  - .nhs.net (NHS mail)
  - .pnn.police.uk (Police)
  - .scn.gov.uk (Criminal and Justice)
  - Emails between Wiltshire Council accounts are secure
  - Any local arrangements
6. In-transit security is reliant on BOTH the sender AND recipient using one of the email domains listed above. In the absence of this, the SENDER will need to encrypt the content of the email using additional software or use a PASSWORD. This may be achieved by sending an encrypted attachment. Other methods include using the, or the NHSmail [SECURE] system. In all transfer scenarios, the onus is on the SENDER to ensure that:
  - Information is transferred securely
  - The chosen method is acceptable to and workable by the recipient
  - Information has reached the required recipient
  - The password used should be a strong - [advice can be accessed here](#).
7. In the event that a recipient receives information by an unsecured route, it is incumbent on the recipient to advise the sender and agree a secure route for future transfers of information.

## 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
- 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 must be included on all forms.

### Benefits of the intended sharing

By ensuring all members of the WSAB 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:

**Approved by (Signatory Name):** .....

**Signature:** .....

**For (Member Organisation):** .....

**Date:** .....

**Once signed, this document should be sent to the Wiltshire Safeguarding Adults Board. Copies should be retained by the named person above and be made available for inspection. A copy should also be sent to the Data Protection Officer/ Caldicott Guardian of each partner organisation, if this is a different person.**

## Appendix 1

### Flow chart of when and how to share information

