

Solihull Safeguarding Adults Board Information Sharing Agreement 2023- 2025

pushing
bullying
pinching
withholding food & drink
coercion
intimidation
hitting
isolating
emotional abuse
restraint
shaking
misusing medication
scalding
teasing
sexual abuse
leaving on own
blaming
stealing money or benefits
neglect
leaving on own
ignoring needs

Contents

	Page no
1 Deciding what information needs to be shared	3
2 Fairness and transparency	13
3 Information quality standards	15
4 Retention of shared information	17
5 Security of shared information	18
6 Access to personal information & Freedom of Information	20
7 Review	21
8 Signatories	22
9 References	27

Version Control

Title	Information Sharing Agreement between Solihull Safeguarding Adults Board and member organisations
Document type	Draft
Prepared by:	Solihull Safeguarding Adults Board Business Team
Approved by	Unapproved at present
Review date:	Every 2 years or if legislation changes
Circulation	Signatory authorities to the Information Sharing Agreement

Version History		
Version Number	Date	Description
1.0	November 2011	Draft created by Sue Walton SSAB Business Manager and sent to SMBC and member organisations of the Solihull Safeguarding Board for comment
2.0	09 July 2015	Reviewed and revised to ensure compliant with the Care Act 2014
2.1	05 August 2015	Changes identified by Andrew Shipway SMBC Corporate Information Governance Manager
2.2	4 th January 2016	Changes made following comments received from CCG, West Midlands Police, Age UK Solihull and BSMHFT.
3.0	Sept 2019	Review
3.1	January 2021	Changes identified by Nigel Parr BSOL CCG Senior Information Governance Manager and Andrew Shipway SMBC Corporate Information Governance Manager
3.2	January 2021	Circulated for signatures
3.2	June 2021	SSAB meeting 10 th June 2021
4.0	March 2023	Review

1. Deciding what information needs to be shared

The Data Protection Act requires that any sharing of personal information must be necessary. Any information shared must be relevant and not excessive.

1.1 Objectives

- 1.1.1 This Information Sharing Agreement sets out the principles for using and sharing personal information amongst the member organisations of Solihull's Safeguarding Adults Board (SSAB).
- 1.1.2 To support earlier identification, prevention, investigation/enquiry and treatment of abuse of adults with care and support needs, the Safeguarding Adults Board is heavily reliant on all partner agencies sharing a variety of relevant information. Effective and structured sharing of information between partners will inform planning, allow for an understanding of trends and patterns of activity to be developed, to respond to emergencies and disasters appropriately, and to intervene and support the wellbeing and safety of individuals, families and communities.
- 1.1.3 Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal information is lawful, properly controlled and that an individual's rights are respected. This must however be balanced with the need to share information to provide safe quality services, to protect individuals and the wider public and the protection of those individuals confidentiality, with the use and correct application of relevant law and guidance on the sharing of information for a specified purpose as laid out in this document.
- 1.1.4 When processing personal information to support the objectives set out in this Data Sharing Agreement, each signatory will act as a 'data controller', as defined in Data Protection legislation. Each signatory is therefore responsible for ensuring that their processing of personal data complies with Data Protection legislation at all times.

1.2 Risks

- 1.2.1 There are considerable risks if information is not shared as has been identified in National Serious Case Reviews, which from 1st April 2015 are known as Safeguarding Adult Reviews. Not sharing information could result in adults being left at risk of harm and mistreatment, which would have a negative or detrimental effect in the individual's health, wellbeing and safety.
- 1.2.2 The benefits to sharing information within the Safeguarding Adults procedures are effective and proportionate partnership working that will safeguard adults with care and support needs. The benefits of sharing information within the Safeguarding Adults procedures outweigh the risk of not sharing information. Information is not to be shared or accessed at a location outside of the UK.

1.3 Anonymised Information

- 1.3.1 Wherever possible anonymised information should be used: In that, it is not possible to identify the individual from the information. However, there will be times within the Safeguarding Adults procedures where information must be client-identifiable – this will be any information, which can identify a living individual (either by itself or with other information likely to come into someone's possession).
- 1.3.2 The agency disclosing information has a right to expect that the agency receiving the information will treat it according to, or under the same legal basis, as which it was first provided to the disclosing agency.

1.4 Minimum Information Shared

- 1.4.1 Sharing Excessive information that is surplus to requirements will breach Article 5(1)(c) of the General Data Protection Regulation ('Data Minimisation'). Therefore, only relevant information and the minimum necessary to achieve the objective will be shared. This applies to information shared internally and with partner agencies. It applies to information shared verbally, electronically, hard copies such as reports and access to information systems.
- 1.4.2 Section 45 of the Care Act 2015 focuses on 'supply of information'. This relates to the responsibilities of others to comply with requests for information from the Safeguarding Adults Board.
- 1.4.3 The Statutory Guidance to the Care Act 2015 emphasises the need to share information about safeguarding concerns at an early stage.
- 1.4.4 All SAB member organisations are responsible for ensuring that information shared about individuals alleged to have caused harm is in accordance with human rights, data protection and confidentiality requirements.
- 1.4.5 Where a concern has been raised, information may be shared within the Adult Safeguarding: Multi-agency policy and procedures for the protection of adults with care and support needs in the West Midlands, that includes any of the above in addition to, or contained within, the following:
- Reports of a concern where evidence or information has been collated.
 - The agenda, minutes and reports of an Adult Safeguarding meeting
 - Letters of referral to regulatory, indemnifying or representative bodies.
 - Referrals to the Police.
 - Minutes of meetings of the Safeguarding Adult Board.
- 1.4.6 The General Data Protection Regulation contains the following three categories of personal data:
- Personal Data - Information relating to living people who can be identified or are in some way identifiable directly from that data

- Special Category Personal Data - Information considered sensitive under Data Protection legislation (Also see section 1.7 'sensitive information')
- Criminal Convictions - Information relating to an individual's criminal convictions and/or offences (Also see section 1.7 'sensitive information')

Personal information may include:

- The person's name, and/or any aliases they live under.
- The person's address(s), occupation and date of birth.
- Information about the person's social circumstances (which may include references to ethnicity). (Also, see section 1.7 - Sensitive Information).
- Information relating to the person's alleged or proven, past or present criminal offences. (Also, see section 1.7 - Sensitive Information).
- The person's movements, habits, conduct or practises. (Also, see section 1.7 - Sensitive Information).

1.5 What does the law say about sharing information?

1.5.1 Information-sharing is related to a number of different pieces of legislation:

- The Care Act 2014
- The Common Law Duty of Confidentiality
- The Human Rights Act 1998, Article 8 (the right to respect for private life)
- The Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- The Crime and Disorder Act 1998
- The Mental Capacity Act 2005

1.5.2 The Care Act 2014

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
- co-operate with each of its relevant partners; each relevant partner must also co-operate with the local authority.

Section 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.

The statutory guidance to the Care Act emphasises the need to share information about safeguarding concerns at an early stage; information-sharing agreements or protocols should be in place.

All SAB member organisations are responsible for ensuring that information shared about individuals alleged to have caused harm is in accordance with human rights, data protection and confidentiality requirements.

1.5.3 Duty of Candour

Regulations under the Care Act place a duty of candour on all service providers registered with the Care Quality Commission from April 2015. The duty:

- aims to ensure transparency and honesty when things go wrong
- requires providers to tell the person concerned when something has gone wrong as soon as possible and provide support to them
- includes giving an apology and keeping the person informed about any further enquiries.

1.5.4 The Common Law Duty of Confidentiality

Confidentiality is an important principle that enables people to feel safe in sharing their concerns and to ask for help. However, the right to confidentiality is not absolute. Sharing relevant information with the right people at the right time is vital to good safeguarding practice.

All staff and volunteers should be familiar with their internal safeguarding procedures for raising concerns. They can also contact either the police or the local authority safeguarding lead for advice, without necessarily giving an individual's personal details, if they are unsure whether a safeguarding concern should be raised.

Some basic principles:

- Don't give assurances about absolute confidentiality.
- Try to gain consent to share information as necessary.
- Consider the person's mental capacity to consent to information being shared and seek assistance if you are uncertain.
- Make sure that others are not put at risk by information being kept confidential.
- Does the public interest served by disclosure of personal information outweigh the public interest served by protecting confidentiality?
- Could your action prevent a serious crime?
- Don't put management or organisational interests before safety.
- Share information on a 'need-to-know' basis and do not share more information than necessary.
- Record decisions and reasoning about information that is shared.
- Carefully consider the risks of sharing information in relation to domestic abuse or hate crime.
- Inform Individuals about how their confidential information is used.

1.5.5 The Caldicott principles

The sharing of information in health and social care is guided by the Caldicott principles. These principles are reflected in the Data Protection Act and are useful to other sectors:

- Justify the purpose(s).

- Don't use personal confidential data unless it is absolutely necessary.
- Use the minimum personal confidential data necessary for purpose.
- Access to personal confidential data should be on a strict need-to-know basis.
- Everyone with access to personal confidential data should be aware of their responsibilities.
- Comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.

1.5.6 **The Human Rights Act 1998**

- Under Article 8 of the European Convention on Human Rights, individuals have a right to respect for their private life.
- This is not an absolute right and can be overridden if necessary and in accordance with the law.
- Interference must be justified and be for a particular purpose.
- Justification could be protection of health, prevention of crime, protection of the rights and freedoms of others.
- A decision to share information and the reasoning behind it should be recorded.

1.5.7 **The UK General Data Protection Regulation (UK GDPR)**

The UK GDPR is a regulation in EU law on data protection and privacy. It is designed to give individuals control over their personal data and place strict requirements on organisations processing personal data. The UK Government enacted the GDPR's requirements into law via the Data Protection Act 2018.

1.5.8 **The Data Protection Legislation**

The Data Protection legislation controls how your personal information is used by organisations, businesses or the government. It supplements the UK GDPR.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles', which are found within the UK GDPR. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

1.5.9 The Crime and Disorder Act 1998

Any person may disclose information to a relevant authority under Section 115 of the Crime and Disorder Act 1998, 'where disclosure is necessary or expedient for the purposes of the Act (reduction and prevention of crime and disorder)'. 'Relevant authorities', broadly, are the police, local authorities, health authorities (clinical commissioning groups) and local probation boards. "The term necessary imposes a strict requirement because the condition will not be met if the organisation can achieve the purpose by some other reasonable means".

1.5.10 The Mental Capacity Act 2005

'Professionals and other staff need to understand and always work in line with the Mental Capacity Act 2005. They should use their professional judgement and balance many competing views. They will need considerable guidance and support from their employers if they are to help adults manage risk in ways that put them in control of decision-making if possible'.

- The Mental Capacity Act will apply if there is any doubt that the person concerned has the mental capacity to make specific decisions about sharing information or accepting intervention in relation to their own safety.
- The Mental Capacity Act 'Code of practice' states that: 'The person who assesses an individual's capacity to make a decision will usually be the person who is directly concerned with the individual at the time the decision needs to be made'.
- In most cases, a worker should be able to assess whether a person has the mental capacity to make a specific decision – see the two-stage functional test of capacity.

The two-stage functional test of capacity

In order to decide whether an individual has the capacity to make a particular decision, you must answer two questions:

Stage 1: is there an impairment of or disturbance in the functioning of a person's mind or brain? If so,

Stage 2: is the impairment or disturbance sufficient that the person lacks the capacity to make a particular decision?

The Mental Capacity Act states that a person is unable to make their own decision if they cannot do one or more of the following four things:

- understand information given to them
- retain that information long enough to be able to make a decision
- weigh up the information available to make the decision
- communicate their decision – this could be by talking, using sign language or even simple muscle movements such as blinking an eye or squeezing a hand.

Other considerations

- Every effort should be made to find ways of communicating with someone before deciding they lack capacity to make a decision.
- Different methods (e.g. pictures, communication cards or signing) should be used to support people with communication difficulties to make sure their views are heard.
- Family, friends, carers or other professionals should be involved as appropriate.
- The mental capacity assessment must be made on the balance of probabilities – is it more likely than not that the person lacks capacity?
- You must be able to show in your records why you have come to your conclusion that capacity is lacking for the particular decision in question.

1.5.11 Sharing information on those who may pose a risk to others

The police can keep records on any person known to be a target or a potential source of harm and share such information with safeguarding partners for the purposes of protection 'under Section 115 of the Crime and Disorder Act 1998, provided that criteria outlined in the legislation are met'. All police forces now have IT systems in place to help identify repeat and vulnerable victims of antisocial behaviour.

1.6 Restrictions on sharing information

- 1.6.1 Parties to this agreement have not identified any legislation that will prevent the lawful sharing of relevant information.

1.7 Sensitive Personal Information

- 1.7.1 The threshold for sharing sensitive personal information is generally higher than for sharing other forms of information. This is because the unnecessary or inappropriate sharing of this sort of information is more likely to cause damage, distress or embarrassment to individuals. Sensitive personal information is defined for the purposes of this data sharing agreement as 'special category' personal data found at Article 9(1) of the UK GDPR and personal data relating to criminal convictions and offences (Article 10 for the UK GDPR). Special category personal data includes the following where it relates to an identifiable individual:

- (a) Racial or Ethnic Origin.
- (b) Political Opinions.
- (c) Religious or Philosophical Beliefs or other beliefs of a similar nature.
- (d) Trade Union Membership or Affiliation.
- (e) Genetic and biometric data;
- (f) Physical or Mental Health or Condition.
- (g) Sexual Life or sexual orientation.

- 1.7.2 Having considered the above, within Safeguarding procedures for the protection of adults with care and support needs in the West Midlands, it may

be essential that this information is shared to allow partners to effectively work together to safeguard adults with care and support needs.

1.8 Consent and Lawful Basis for Processing

- 1.8.1 To process personal data, member organisations must identify and document a lawful basis for processing personal data, consistent with Article 6 of the UK GDPR. There are additional requirements for processing special category personal data or personal data relating to criminal convictions and offences.
- 1.8.2 For the purposes of this data sharing agreement, the lawful basis for processing personal data is Article 6(1)(e) where the processing is necessary to perform a task in the public interest and the task and function has a clear basis in law. The personal data shared under this agreement is designed to satisfy member organisations' obligations and responsibilities under Safeguarding legislation.
- 1.8.3 The lawful basis for processing special category personal data is Article 9 (2) (g) of the UK GDPR where the processing is necessary for the purposes of substantial public interest (protection of vulnerable individuals) in combination with section 10 (3) and Schedule 1, Part 2, condition 18 of the Data Protection Act 2018 ('processing is necessary for the purposes of protection of adults at risk').
- 1.8.4 The lawful basis for processing criminal convictions data is found at Article 10 UK GDPR in combination with Schedule 1, Part 2, condition 10 ('preventing or detecting unlawful acts'), condition 18 ('processing is necessary for the purposes of protection of adults at risk'), and/or condition 6 ('where the processing is for the exercise of a function conferred on a person by an enactment or rule of law').
- 1.8.5 The processing of personal data for safeguarding purposes should not rely on consent unless it is absolutely necessary. Gaining the consent of the individuals' whose information you want to share will often help legitimise the sharing of personal information, however it is not always appropriate to use consent as the basis for sharing information, the following justifications under Safeguarding Adults may become applicable:
- **Serious harm**
It may be justified to share information where there is evidence that serious harm would be caused to the service user, (or another person) if this was not done.
 - **Vital interests**
Information may be shared where this is in the "vital interests" of the service user or another person. This refers to life or death circumstances.
 - **Prevention or detection of crime**
Personal information may be provided to the Police where this is necessary for the prevention or detection of crime. This is a power not an obligation. A judgement needs to be made in each case as to whether it

is appropriate to release information taking into account the following criteria.

- Without disclosure the task of preventing or detecting crime would be seriously prejudiced, and
- Information shared is limited to what is strictly relevant to a specific investigation, and
- There are satisfactory undertakings that the information will not be used for any other purpose than the specific investigation.

Advice should be sought, if there is uncertainty about interpreting this criteria.

- **Court Order**

Information must be shared where the service is instructed to do so by a Court (including a Coroner's Court.)

- **Legislation**

The law requires or permits the information to be shared.

Wherever possible and appropriate, service users should be informed if their information is to be shared without consent.

Informed consent

- 1.8.6 If at any time it is decided that consent is needed, this must be a specific, informed and freely given agreement. In this context, a failure to object is not consent. Most importantly, the individual must understand what is being consented to and the consequences of giving or withholding consent. All relevant record keeping systems should record the outcome of the request for consent.

Withdrawn consent

- 1.8.7 If consent is being relied upon to share information about a person, then sharing must stop if consent expires or is withdrawn. All relevant record keeping systems should record the outcome of the request for consent.

Special Category (Sensitive) Data

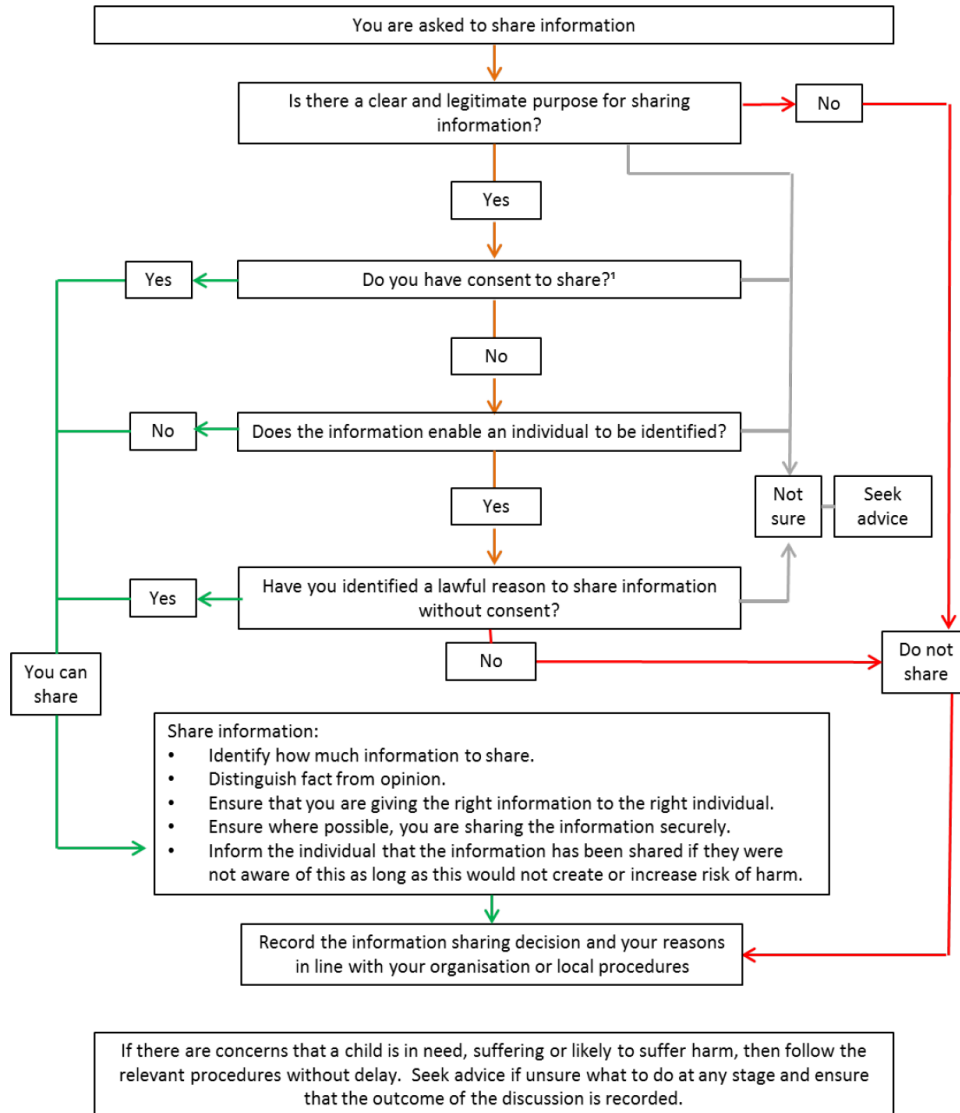
- 1.8.8 If the information to be shared is sensitive, then if consent is relied upon it must be 'explicit' consent. This difference between normal consent and explicit consent is that with explicit consent, the consent of the individual must be absolutely clear and ideally consent will be obtained in writing. All relevant record keeping systems should record the outcome of the request for consent.

1.8.9 **Sharing information with carers, family or friends**

It is good practice, unless there are clear reasons for not doing so, to work with the carers, family and friends of an individual to help them to get the care and support they need. Sharing information with these people should always

be with the consent of the individual. If the person lacks the mental capacity to make a decision about sharing information with key people, then the Mental Capacity Act should be followed to ensure each decision to share information is in the person's best interests. Decisions and reasoning should always be recorded.

Flowchart for when and how to share information



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

This flowchart is taken from HM Government Information sharing - Advice for practitioners providing safeguarding services to children, young people, parents and carers July 2018 – also applicable for Adult Safeguarding.

2. Fairness and transparency

The Data Protection Legislation (Chapter III of UK GDPR) requires that with some exceptions, in order for the information sharing to be 'fair' the individuals' whose information is being shared need to be made aware of the fact that the exchange is taking place, by whom and why.

2.1 Privacy Notices

2.1.1 The UK GDPR requires that the organisation in charge of processing personal information, should provide or make readily available the following information:

- The contact details of their data protection officer (if applicable).
- The purposes of the processing.
- The lawful basis for the processing.
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority (e.g. Information Commissioner's Office).
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

2.1.2 How you inform people of the above will depend upon the circumstances, for example, it might be a statement on a form, or it might be put on an organisations website or perhaps delivered verbally if circumstances warrant this.

Note: There is a fundamental difference between telling a person how you're going to use their personal information and getting their consent for this. In many cases, a privacy notice will suffice. In cases where sensitive personal information is involved, positive (often written) consent will be needed.

2.1.3 Members of the Safeguarding Board agree to ensure that when collecting information from individuals they provide the information described above.

3. Information quality standards

The Data Protection Act requires that personal information be relevant, kept accurate and up to date. Decisions taken on inaccurate information can have serious consequences.

3.1 Six Elements of Information Quality

3.1.1 Signatories to this agreement have no desire to share inaccurate information. Parties are in agreement that any information shared should be of the highest quality and that procedure/systems will be in place to guarantee this. The 6 elements to Information Quality agreed upon are:

- 1 **Accurate** Information should be sufficiently accurate for its purposes. The need for accuracy must be balanced with the importance of the uses for the information, and the costs and effort of collection. Sometimes it may be acceptable to have some degree of inaccuracy. However, where compromises have to be made on accuracy, this should be made clear.
- 2 **Valid** There may be national or local rules to follow. Different organisations may record the same information in different ways. For example, a person's date of birth can be recorded in various formats. This can lead to records being mismatched or becoming corrupted. Before sharing information you must make sure that the organisations involved have a common way of recording key information.
- 3 **Reliable** The methods used to gather information should remain consistent as users of the shared information need to be confident that any differences reflect real change rather than differences generated by different collection methods.
- 4 **Timely** Information should be shared as quickly as possible after being captured else it may become out of date and obsolete. The speed and frequency at which you share the information will depend upon how likely it is to change over time.
- 5 **Relevant** Information should be relevant to the purposes for which it is shared. The accuracy of information and methods used to collect/generate it may be excellent and fulfill all parties' needs today, however, tomorrow, there may be new requirements or rules introduced that have to be adhered to and mean that you have to review the information collected.

6 Complete Information requirements should be clearly specified. Methods of collecting the information need to meet these requirements else the information may be incomplete. It is vital that those responsible with collecting or creating information are all clear about why the information is being shared and the purposes it will be used for else the wrong information might be shared.

3.2 Each SAB member organisation must have arrangements in place so the correction of data quality inaccuracies can be notified and undertaken.

4. Retention of shared information

It is a Data Protection principle that personal information should not be kept for any longer than is required.

- 4.1.1 Parties to this agreement understand that the information shared should not be held indefinitely and should only be retained for as long as it is needed. The retention period will either be based upon legislation, which requires that the information be kept for a set period, or in the absence of any legislative requirement, each party to this agreement will determine how long they need to keep the information based upon their own business need.
- 4.1.2 After this time the information will be permanently deleted and this will apply both electronic and manual records.
- Electronic Records – For information to be deleted it must be permanently and irrecoverably deleted. This means it cannot exist on the organisations electronic backups or other systems, unless it is held for different purposes, which require it to be retained for longer. Advice and assurance should be sought from the relevant IT provider to make sure that non-recovery deletion of record has happened to industry standard.
 - Manual Information – Each party to this agreement holds manual information on service users. Each service user has a manual file (similar to a personnel file). In line with the above retention schedule, each party has agreed that the file will be shredded and put into confidential waste at the end of the retention period. Shredding of documents should be at least at a minimum industry standard level of DIN4 (cross-shredded).

It is perfectly permissible for parties to this agreement to have different requirements for how long they keep the information shared. This is because different organisations will be working under different legislation or have differing business needs.

5. Security of shared information

The Data Protection legislation requires that organisations have adequate organisational and technical safeguards in place to guarantee the safety and security of personal information they hold. Any safeguards must be proportional and appropriate to the nature of the information and the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage.

5.1 General principles

Members of the Safeguarding Board agree that personal information shall be protected by appropriate technical and organisational measures including the agreement that:

5.1.1 Identify/Evaluate Risk

Information to be shared is generally highly sensitive and the damage that could result by accidental loss or disclosure is significant. Therefore, a high level of security and safeguards needs to be in place to manage the risk of accidental loss or disclosure. Information will only be accessed by those who need to know it.

5.1.2 Protective Markings

A difficulty that can arise when information is shared is that the various organisations involved can have different standards of security and security cultures. Adopting the Government Protective Marking Scheme can help organisations involved in the sharing of information to make sure there is consistency when handling personal information.

Due to the sensitive and confidential nature of Safeguarding Adults information, the Government Protective Marking of OFFICIAL-SENSITIVE [PERSONAL] should be applied to the information shared. This is on the basis that loss or misuse would:

- Pose a risk to an individual's personal safety or liberty.
- Facilitate the commission of, or impede the investigation or prosecution of low-level crime.
- Directly lead to a risk to an individual's personal safety (e.g. the compromise of the address of a victim of abuse, where there is a reasonable risk of further abuse if such information became known).
- Cause either prolonged distress for an individual, or short-term distress or significant embarrassment for many individuals.

Any information shared should be clearly marked as OFFICIAL-SENSITIVE [PERSONAL].

Note: Guidance will be issued in the autumn regarding changes to Protective Marking.

5.2 Physical Mechanisms for delivering/sharing the information

Electronic Sharing of Information

5.2.1 Any information that is shared electronically must be done so via encrypted means. For example if information is shared by email then it will not be sufficient to simply password protect a document, the email itself must be encrypted. Alternatively, the email can be sent via a secure network such as the GCSX network.

Postal Service

5.2.2 If information is sent through the post, it will be sent by special delivery. Items sent by Special Delivery are tracked throughout their journey through the postal system and so if they get lost there is a stronger chance they will be found. Items sent by Recorded Delivery is treated as normal post except for the fact they are signed for upon delivery. Therefore, Recorded Delivery will not be used.

5.2.3 Parties to this agreement will ensure that the envelopes/packaging used are either special tamper proof packaging or else strong enough to prevent damage and potential loss of information during transit.

6 Access to personal information and Freedom of Information

Art 15 UK GDPR gives individuals the right to ask for and receive copies of personal information held by an organisation (subject to certain exemptions) and the Freedom of Information Act 2000 gives individuals rights of access to all other types of information

6.1 How to Handle requests for Information

- 6.1.1 All parties to this agreement have agreed that if any organisation receives a request from an individual to access any of the shared information, it is their responsibility to process the request. However, should the information in question have originated from another organisation then they will be contacted within 5 days of receiving the request and views sought on whether the information should be disclosed or whether there are any reasons which would legitimise it being withheld.
- 6.1.2 If a member of the public requests a full copy of the signed information sharing agreement, parties to this agreement should generally not have any objections to a full copy being released, as ordinarily this information would be available by way of their publication schemes.
- 6.1.3 Safeguarding Adults Boards are not defined as Public Authorities for the purposes of the Freedom of Information Act 2000 and are not therefore subject to rights of access to information.

7 Review


7.1 Annual Reviews


7.1.1 This Information Sharing Agreement will be reviewed by all parties on the anniversary of the signing of this agreement. Thereafter, it will be reviewed at least annually or sooner should circumstances warrant it.


7.1.2 Each review will examine whether:


- The sharing of information is having the desired effect.
- Fair processing notices still provide an accurate explanation of the information sharing activity.
- Procedures for ensuring the quality of information are being adhered to and are working in practice.
- Organisations you are sharing information with are also meeting agreed quality standards.
- Retention periods are being adhered to and continue to reflect business need.
- Security remains adequate and, if not, whether any security breaches have been investigated and acted upon.
- Individuals are being given access to all the information they are entitled to, and that they are finding it easy to exercise their rights.

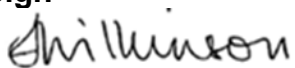
8 Signatories


Solihull MBC	Name Lizzie Edwards Assistant Director
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 3 rd April 2023


West Midlands Police	Name Andy Beard Chief Superintendent - Solihull NPU
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 20 th March 2023


Birmingham & Solihull Integrated Care Board	Name Lisa Stalley-Green Deputy CEO / Chief Nursing Officer
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 23 rd March 2023

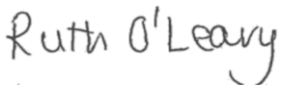
Age UK Solihull	Name Anne Hastings Chief Executive Officer
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 31 st March 2023


Birmingham & Solihull Mental Health Foundation Trust	Name Jane Wilkinson Interim Head of Safeguarding
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 31 st March 2023


Carers Trust Solihull	Name Brandon Scott-Omenka Chief Executive Officer
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 25 th July 2023

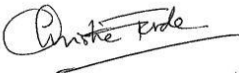
Coventry and Warwickshire NHS Partnership Trust	Name Mary Mumvuri Chief Nursing Officer Safeguarding Team
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 26 th July 2023


Healthwatch Solihull	Name Andy Cave Chief Executive Officer
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 25 th July 2023


University Hospitals Birmingham	Name Ruth O'Leary Director of Safeguarding & Vulnerabilities
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 31st March 2023

Probation Service	Name Neil Appleby Head – Probation Service
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 6th April 2023

Provider Representative	Name Alka Sahnun Registered Manager Prince of Wales Nursing Home
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date: 3rd August 2023

Solihull Action through Advocacy	Name: Christine Forde
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 26 th July 2023

Solihull Community Housing	Name Carol Trappett Head of Housing & Neighbourhood Services
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 6 th April 2023

West Midlands Fire and Rescue Service	Name
I have read the Information Sharing Agreement and on behalf of my organisation, I agree to implement the terms and conditions of this Agreement and confirm that we have read and understood the indemnity agreement.	
Sign 	Date 2 nd May 2023

References

- UK Legislation - Care Act 2014
- Department of Health - Care and Support Statutory Guidance Issued under the Care Act 2014 (October 2014)
- Department of Health - Statement of Government Policy on Adult Safeguarding (10 May 2013)
- Adult Safeguarding: Multi-agency policy & procedures for the protection of adults with care & support needs in the West Midlands (1st November 2019)
- HM Government Information sharing - Advice for practitioners providing safeguarding services to children, young people, parents and carers - July 2018