LOCAL SAFEGUARDING ADULTS BOARD

INFORMATION SHARING AGREEMENT

October 2026

Status

Revised draft for legal, data protection and partner assurance before Board approval.

Document control	Detail
Owner	LSAB Executive Group
Author	LSAB Board Manager
Information Asset Owner	Jennifer Harrison
Approval body	Local Safeguarding Adults Board
Approval date	September 2026
Publication date	October 2026
Status	Approved – final version
Version	6
Approved document location	LSAB controlled document repository

Document control	Detail
Review cycle	Every two years, or earlier following a material legal, regulatory, technological, or operational change
Next scheduled review	October 2028
Review owner	LSAB Board Manager

This agreement must not be treated as legal advice for an individual case. Practitioners must use professional judgement, follow their organisation's procedures, and seek timely advice where necessary.

Version history

Version	5	Summary	Author / approver
2	June 2026	Earlier draft	LSAB Board Manager
3	July 2026	Draft reviewed for Board-level assurance	LSAB Board Manager
4	July 2026	Rewritten to strengthen legal basis mapping, governance, accountability, AI controls, decision records, and current legislative alignment	LSAB Board Manager / subject to assurance
5	August 2026	Expanded in plain language to address confidentiality, information rights, lawful basis, criminal offence data, Caldicott, records, governance and operational recommendations	LSAB Board Manager / subject to assurance
6	October 2026	Final version approved by Local Authority Information Governance Manager	Approved at Executive

Approval and sign-off

Role	Name	Assurance / approval	Date
LSAB Chair	Ceila Jeffreys	Approval	Sep-26
LSAB Board Manager	Dawn Lewis	Assurance	Oct-26

Role	Name	Assurance / approval	Date
Responsible senior officer / Information Asset Owner	Jennifer Harrison	Approval	Sep-26
Data Protection Officer / information governance lead	Phil Orchard	Approval	Oct-26
Adult social care	Stella Higgin	Approval	Oct-26
Caldicott Guardian / health IG representative	Sarah Martin	Approval	Oct-26
Police data protection representative	Michelle Thompson	Approval	Oct-26

Contents

1. Foreword and status of this agreement

1.3 How to use this agreement

This agreement uses plain language. It tells staff what they must check before sharing information, what they must record, and when they must ask for advice. It does not replace the law, professional judgement or an organisation's own procedures. If the position is unclear or the risk is high, staff must seek advice promptly and must not allow avoidable harm to continue.

2. Purpose, scope, and outcomes

3. Core principles and practitioner rules

3.4 Caldicott Principles

Partners handling confidential health or social care information must apply the eight Caldicott Principles. These principles must be considered in every relevant request, disclosure, system design, audit and review.

1. Justify the purpose for using confidential information.
2. Use confidential information only when it is necessary.
3. Use the minimum necessary confidential information.
4. Give access only on a strict need-to-know basis.
5. Make sure everyone understands their responsibilities.
6. Comply with the law.
7. Recognise that the duty to share information for individual care can be as important as the duty to protect confidentiality.
8. Inform people about how their confidential information is used, unless the law allows information to be delayed or withheld.

For novel, difficult or high-risk decisions involving health or social care information, staff should involve the Caldicott Guardian or equivalent senior adviser. Appendix B must record the relevant Caldicott considerations.

4. Legal and ethical framework

4.6 Statutory gateways and restrictions

A statutory gateway is a legal power or duty that may allow or require information to be shared. It is not a blanket permission. The decision-maker must identify the exact provision, check that its conditions are met, and share only what is necessary. A power to request information does not always create a duty to disclose it.

- Care Act 2014 sections 6 and 7 supports cooperation, but do not remove the need to consider data protection, confidentiality and human rights.

- Section 42 supports enquiries where all statutory criteria are met. The information shared must be relevant to the enquiry or protective action.
- Section 44 supports Safeguarding Adults Reviews. Identifiable information must still be necessary for the review purpose.
- Section 45 allows a Safeguarding Adults Board to request information when the statutory conditions are met. It is not the routine gateway for every operational disclosure.
- Other gateways may arise under health and social care law, crime and disorder law, court powers, regulatory duties, professional referral duties or a valid court order. The exact provision must be recorded.
- Where a legal restriction, sealing order, privilege, statutory bar or specific confidentiality rule applies, staff must obtain advice before disclosure unless immediate lawful action is required to protect life or prevent serious harm.

4.7 Public-interest disclosure and sharing without consent

A person's refusal or lack of agreement does not automatically prevent information sharing. It also does not automatically make sharing lawful. The decision-maker must separately identify the data protection basis, the confidentiality basis, any statutory power or duty, and the human rights justification.

Where overriding public interest is relied upon, the record must explain:

- what harm, abuse, neglect, crime or serious risk is being addressed;
- how serious, likely and urgent the risk is;
- whose rights or safety require protection;
- why sharing is likely to help;
- why a less intrusive action or narrower disclosure would not be enough;
- what information and recipients are strictly necessary;
- what risks sharing may cause, including retaliation, distress or loss of trust; and

- why the public interest in sharing outweighs the duty of confidence in the particular case.

Information may be shared without consent where the test is met, including where this is necessary to protect the person or others, carry out a statutory safeguarding function, prevent or detect serious crime, comply with a court order, or meet another overriding public interest. The decision must not rely only on labels such as “safeguarding” or “public interest.”

4.8 Professional confidentiality obligations

Staff must follow the confidentiality rules that apply to their profession, role, contract and employer. This may include standards issued by health, social work, legal, policing or other professional bodies. Professional rules do not replace the law, but they may require a higher standard of justification, consultation, record keeping or escalation. Where duties conflict or the position is uncertain, staff must seek advice from their professional lead, legal adviser, DPO or Caldicott Guardian as appropriate.

4.9 Criminal offence data

Criminal offence data includes convictions, alleged offences, suspected offending, proceedings, acquittals and related security measures. It must be clearly distinguished from fact, allegation, intelligence and professional opinion.

Before processing or sharing criminal offence data, the controller must identify and record:

- the Article 6 lawful basis;
- whether the processing is under official authority or is authorised by UK law;
- the exact Data Protection Act 2018 condition relied upon;
- whether an appropriate policy document is required and is current;
- whether the organisation is acting as a competent authority for a law-enforcement purpose, meaning Part 3 of the Data Protection Act 2018 applies;
- why the processing is necessary and proportionate;
- whether a DPIA is required;

- who may have access and how the information will be protected;
- how accuracy, review, correction and retention will be managed; and
- how unfairness, stigma and unsupported conclusions will be prevented.

No partner may create or maintain a comprehensive register of criminal convictions unless it has the legal authority to do so. Information about an allegation, arrest, charge, conviction, acquittal or intelligence assessment must not be presented as if these categories mean the same thing.

5. Parties, roles, and accountability

5.4 Record roles and responsibilities

For each routine data flow, Appendix C must identify the originating organisation, source controller, receiving controller, any processor, and the organisation responsible for the authoritative or master record. “Record ownership” in this agreement means operational responsibility for a record. It does not remove another controller’s legal duties for the copy it holds.

- The originating organisation is responsible for the accuracy and context of information when it sends it and for notifying known material corrections.
- An independent receiving controller is responsible for its own copy, use, security, access, retention, disclosure, accuracy notes and response to rights requests.
- A receiving controller must not silently alter the originating organisation’s account. It may correct its own factual errors and add a clear note, challenge or later update.
- A processor must act only on the controller’s documented instructions and under a compliant written contract.
- The organisation responsible for the master record must keep the main record complete, reliable and auditable.

- Each organisation must preserve the history of material corrections and must communicate relevant corrections, restrictions or risk updates to known recipients without undue delay.

6. Permitted purposes, information, and recipients

6.5 When a supplementary operational sharing agreement is required

The main agreement does not authorise an undocumented routine data flow. An approved Appendix C schedule, or an equivalent supplementary operational agreement, is required before routine, repeated, bulk, matched, linked, shared-system or system-to-system sharing begins.

The supplementary arrangement must cover the data flow, roles, lawful bases, confidentiality, rights, security, retention, data quality, incident handling, audit and approvals. Depending on the arrangement, partners may also need a DPIA, joint-controller arrangement, processor contract, system-access agreement, technical specification or international-transfer assessment. A one-off case disclosure will normally use Appendices A and B. An emergency disclosure may proceed where necessary but must be recorded and reviewed as soon as practicable.

7. Decision-making, consent, capacity, and confidentiality

8. Operational sharing arrangements

9. Transparency and individual rights

9.1 Privacy information

Each controller must provide clear, accessible privacy information. It must explain who the controller is, why information is used, the lawful bases, the types of information, recipients, retention, rights, complaint routes, international transfers and any relevant automated processing. Partners must use formats that meet communication and accessibility needs.

Where personal data was not obtained from the person, the controller must provide the required information within the legal timescale unless a lawful exception applies. Information may be delayed or limited only to the extent necessary. The reason, scope and review date must be recorded.

9.2 Recognising and coordinating information-rights requests

Staff must promptly send any request about a person's information to their organisation's information-rights team. A request does not need to mention data protection law or use a standard form. Each controller remains responsible for requests about information under its control unless a joint-controller arrangement lawfully allocates operational tasks differently.

Partners must keep current rights-request contacts and cooperate early enough to meet legal timescales. Consultation does not transfer legal responsibility and does not give another organisation a veto.

9.3 Subject access requests

Each controller must search for, review and respond to personal data it controls. Where information came from another partner, the responding controller should consult that partner where reasonably needed to understand context, identify risks, check accuracy, consider third-party information or assess an exemption. The responding controller must make its own final decision.

Safeguarding records must not be withheld as a whole simply because they are sensitive. The controller must consider what can be disclosed safely, whether redaction is sufficient, and whether any specific exemption applies to particular information.

9.4 Rectification and disputed information

A request to correct information must distinguish between:

- an objectively inaccurate fact;

- incomplete or misleading information;
- an accurately recorded allegation;
- an accurately recorded professional opinion;
- information that was accurate at the time but has since changed; and
- a genuine disagreement about interpretation or judgement.

Confirmed factual errors must be corrected without undue delay. An allegation or professional opinion should not be deleted merely because it is disputed if the record accurately shows what was said or believed at the time. Instead, the challenge, evidence, decision and later outcome must be clearly recorded. Material corrections must be sent to relevant recipients where required, while preserving an audit trail.

9.5 Restriction of processing

Requests to restrict processing must be assessed promptly. Where a restriction applies, the organisation must mark the record clearly, limit use as required, tell relevant staff and systems, and notify partner recipients where required. Before lifting a restriction, the person must be informed where the law requires this. A safeguarding concern does not automatically defeat a restriction request; the legal test and reasons must be documented.

9.6 Objections to processing

A person may object to processing in circumstances allowed by law. The controller must identify the lawful basis, consider the person's reasons, assess whether compelling legitimate grounds or legal claims justify continuing, and record the outcome. An objection must be taken seriously even where processing continues for a lawful safeguarding reason.

9.7 Information supplied by partner organisations

When a rights request covers information supplied by another organisation, the responding controller should consult the source organisation where this is necessary and practicable.

Consultation should ask about context, accuracy, professional confidentiality, third-party information, risk and possible exemptions. The source must reply promptly and explain its concerns. The responding controller remains responsible for the decision and statutory response.

No partner should promise that another organisation will disclose or withhold information. Routine data-flow schedules must identify which organisation leads searches, consultation, correction notifications and communication with the person.

9.8 Third-party information

The controller must consider the rights and safety of other people named or identifiable in the record. It must consider consent where appropriate, reasonable expectations, the person's relationship to the requester, confidentiality, risk of harm, whether the source was a professional acting in that role, and whether redaction or a summary would allow safe disclosure. The decision must be case specific.

9.9 Safeguarding-related exemptions and restrictions

An exemption or restriction may be used only where the law allows it and only to the extent necessary. The decision record must identify the legal provision, the information affected, the harm or prejudice being prevented, the reasoning, the review date where relevant, and the information that can still be provided. Blanket policies that automatically withhold all safeguarding information are not permitted. Complex cases must be referred to the DPO, information-rights lead or legal adviser.

9.10 Erasure, portability and automated processing rights

Where relevant, controllers must also assess requests for erasure, data portability, human intervention, explanation or challenge to automated processing. These rights do not all apply in every safeguarding context. The organisation must explain clearly whether the right applies and the reasons for its decision.

9.11 Complaints

Each organisation must provide an accessible data protection complaints process. Complaints must be acknowledged, investigated fairly, answered within the applicable timeframe and signposted to the Information Commissioner. Cross-partner complaints must be coordinated without hiding the accountability of each controller.

9.12 Freedom of Information and Environmental Information requests

Each public authority must decide requests under the Freedom of Information Act 2000 or Environmental Information Regulations 2004 for information it holds. The authority must identify the correct legal regime and consider any exemption or exception case by case.

- Consult the information originator early where this may help explain sensitivity, confidentiality, prejudice or factual context.
- The originator may give reasons, but it does not make the decision and does not have a veto.
- Protective markings and confidentiality labels are relevant context but do not automatically determine the outcome.
- Personal data requests may need to be handled under data protection rights rather than FOI.
- The responding authority must keep a record of its own analysis, public-interest test where required, redactions and final decision.

10. Security, incidents, retention, and disposal

11. Artificial intelligence and automated processing

12. Assurance, escalation, review, and termination

13. Sources and supporting standards

Appendix F: Statutory gateway guide

This guide supports, but does not replace, case-specific legal analysis.

Care Act 2014 sections 6 and 7: Cooperation powers and duties. Record the function being supported and why the information is necessary.

Care Act 2014 section 42: Safeguarding enquiry duty where all statutory criteria are met. Record the criteria, enquiry purpose and minimum information needed.

Care Act 2014 section 44: Safeguarding Adults Review. Use identifiable information only where necessary for the review and learning purpose.

Care Act 2014 section 45: Formal SAB information request where statutory conditions are met. Record the SAB function, conditions, authorisation, recipient, deadline and secure route.

Court order or statutory notice: Check scope, validity, recipient, deadline, restrictions and whether legal advice is required.

Crime prevention, investigation or regulatory referral: Identify the exact power or duty, the controller's role, the applicable data protection regime and the necessity of the proposed disclosure.

Other legal gateways: Record the precise legal provision and obtain advice where the gateway or its conditions are unclear.

Appendix G: Lawful basis decision guide

The lawful basis must reflect the real purpose and legal function. Staff must not choose a basis only because it appears convenient.

- Public task, Article 6(1)(e): commonly relevant where a public body processes information to carry out a task laid down by law or exercise official authority. Record the underlying law or function.

- Legal obligation, Article 6(1)(c): relevant where the controller must process information to comply with a specific legal duty. Record the duty and why processing is necessary.
- Vital interests, Article 6(1)(d): narrow. Use where processing is necessary to protect life or physical integrity and another basis is not available or suitable.
- Consent, Article 6(1)(a): use only where consent is freely given, specific, informed, unambiguous and can be withdrawn without detriment. It is often unsuitable for statutory safeguarding.
- Legitimate interests, Article 6(1)(f): not available to public authorities when carrying out their public tasks. A non-public body must complete and record the required balancing assessment.
- Special category data: identify a separate Article 9 condition and any required Data Protection Act 2018 Schedule 1 condition and appropriate policy document.
- Health or social care condition: use only where the processing genuinely concerns health or social care provision, system management or a related purpose and the legal requirements are met.
- Substantial public interest and safeguarding conditions: identify the exact Schedule 1 condition, show necessity and meet any policy-document requirement.
- Criminal offence data: apply section 4.9 and record Article 10 or Part 3 Data Protection Act 2018 requirements as applicable.

Appendix A: Information sharing request form

Appendix B: Information sharing decision and disclosure record

Appendix C: Data flow and legal basis schedule

Appendix D: Practitioner decision pathway

Appendix E: Partner signatories

1. Foreword and status of this agreement

Safeguarding adults requires effective, timely and lawful information sharing between professionals and organisations. This agreement provides a consistent framework for defensible decisions that protect people from abuse or neglect while respecting privacy, autonomy, dignity, and human rights.

The agreement supports, but does not replace, case-specific professional judgement, legislation, statutory guidance, court orders, professional duties, organisational procedures, or specialist legal and information governance advice.

> **Essential limitation**
> Signing this agreement does not make a disclosure automatically lawful and does not create a blanket gateway for access. Each organisation remains accountable for the information it collects, discloses, receives, and subsequently uses.

1.1 Status and application

- This agreement applies to LSAB partner organisations, their staff, contractors, office holders, and volunteers when sharing information for the purposes set out in section 6.
- It covers planned, routine, ad hoc and urgent sharing, including sharing for safeguarding enquiries, Safeguarding Adults Reviews, quality assurance, prevention, commissioning, and strategic oversight where personal data is required.
- It does not apply to information that has been effectively anonymised so that no living person is identifiable by reasonably likely means. Pseudonymised information remains personal data.
- Where a partner's own policy sets a higher protective standard, that standard should be followed unless it would unlawfully frustrate a safeguarding duty or power.

1.2 Definitions

Term	Meaning
Adult with care and support needs	A person whose circumstances may engage adult care and support functions. The Care Act section 42 duty applies only where all statutory criteria are met.
Adult at risk	A procedural shorthand. It must not replace consideration of section 42 criteria or the person's individual circumstances.
Personal data	Information relating to an identified or identifiable living person.
Special category data	Data within Article 9 UK GDPR, including health, racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic data, biometric identification data, sex life, and sexual orientation.
Criminal offence data	Personal data relating to criminal convictions, alleged offences, proceedings, related security measures, or suspected offending. It is governed by Article 10 UK GDPR and relevant DPA 2018 provisions, not Article 9.
Controller	The person or body that determines the purposes and means of processing.
Joint controllers	Two or more controllers that jointly determine purposes and means and must allocate responsibilities transparently.
Processor	A person or body processing personal data on behalf of a controller under written instructions.

Term	Meaning
Recipient	A person or body to whom personal data is disclosed.
Personal data breach	A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
AI system	A machine-based system that generates outputs such as predictions, content, recommendations, or decisions from inputs.
DPIA	A Data Protection Impact Assessment used to identify and reduce high risks to people before processing begins or materially changes.

2. Purpose, scope, and outcomes

2.1 Purpose

This agreement enables partners to share the minimum necessary information for defined safeguarding and related public-interest purposes in a fair, lawful, transparent, accurate, timely and secure way.

2.2 Intended outcomes

- Prevent death, serious harm, abuse, and neglect.
- Enable effective section 42 enquiries and other lawful safeguarding activity.
- Support person-led outcomes and Making Safeguarding Personal.
- Protect children, other adults and the wider public where risks extend beyond the individual.

- Identify patterns, organisational abuse, repeat concerns, and emerging risks.
- Enable lawful scrutiny, Safeguarding Adults Reviews, and organisational learning.
- Provide a reliable audit trail and clear accountability across partner boundaries.

2.3 Out of scope

- Unrelated secondary uses that are incompatible with the original purpose.
- Indiscriminate access to another organisation's systems or records.
- Disclosure for curiosity, convenience, employment management, or reputational protection without a proper legal basis.
- Use of identifiable safeguarding information for research, training, publicity, or service development unless separately authorised and governed.
- Entry of personal data into unapproved AI tools or consumer applications.

3. Core principles and practitioner rules

3.1 Eight practitioner rules

9. Be clear about the safeguarding purpose, the expected benefit and the harm that may arise from sharing or not sharing.
10. Identify the correct legal basis before disclosure. Partner status or consent alone is not sufficient.
11. Be open with the person unless doing so is unsafe, impossible, seriously prejudicial to the purpose or otherwise lawfully restricted.
12. Share only information that is necessary, relevant, adequate, accurate and proportionate.
13. Share promptly with people who have a legitimate role and a genuine need to know.
14. Use an approved secure method, verify the recipient, and state any onward-sharing or retention restrictions.
15. Record the decision, including a decision not to share, the reasons, information disclosed, recipient, legal basis, method, and date.

16. Escalate delay, refusal, uncertainty, conflicts of duty, inaccurate information, and suspected breaches without allowing avoidable risk to continue.

3.2 Safeguarding principles

Information-sharing decisions should support empowerment, prevention, proportionality, protection, partnership, and accountability. The person's desired outcomes should inform the response wherever practicable, while recognising that action may still be required to protect the person or others.

3.3 Think Family and wider risk

Practitioners must consider whether children, carers, family members, staff, other adults with care and support needs or the public may be at risk. Concerns about a child must be referred through children's safeguarding procedures without delay. Information must not be withheld solely because the adult does not consent where there is a lawful and proportionate need to protect another person.

4. Legal and ethical framework

4.1 Applicable framework

- Care Act 2014 and Care and Support Statutory Guidance, including sections 1, 6, 7, 42, 44 and 45.
- UK General Data Protection Regulation, as amended.
- Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.
- Data (Use and Access) Act 2025, including current requirements for data protection complaints and automated decision-making safeguards.
- Human Rights Act 1998, particularly respect for private and family life under Article 8 ECHR.
- Mental Capacity Act 2005 and associated Code of Practice.

- Common law duty of confidentiality.
- Freedom of Information Act 2000 and Environmental Information Regulations 2004 where applicable.
- Crime and Disorder Act 1998, health and social care legislation, professional duties, court orders, and other lawful powers relevant to the particular case.
- Law enforcement processing rules in Part 3 DPA 2018 where a competent authority processes for a law enforcement purpose.

4.2 Lawful basis

Before sharing personal data, the disclosing controller must identify and document at least one Article 6 UK GDPR lawful basis. Public authorities will commonly rely on legal obligation under Article 6(1)(c) or public task / official authority under Article 6(1)(e). Vital interests under Article 6(1)(d) is narrow and should generally be used only where needed to protect life or physical integrity and another basis is unavailable. Public authorities must not rely on Article 6(1)(f) for processing carried out in performance of their public tasks.

Where special category data is involved, the controller must also identify an Article 9(2) condition and any associated DPA 2018 Schedule 1 condition. Relevant conditions may include health or social care, substantial public interest, safeguarding of children and individuals at risk, preventing, or detecting unlawful acts and statutory or government purposes. The condition must be appropriate to the actual purpose and facts.

Criminal offence data requires separate consideration under Article 10 UK GDPR and the DPA 2018. It must not be recorded as Article 9 special category data. The controller must identify official authority or an applicable Schedule 1 condition and comply with any requirement for an appropriate policy document.

No basis shopping

The agreement does not authorise practitioners to select the most convenient basis from a list. Routine data flows must be mapped in Appendix C, and exceptional disclosures must record the basis that genuinely applies.

4.3 Data protection principles

- Lawfulness, fairness, and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy and prompt correction.
- Storage limitation.
- Integrity and confidentiality.
- Accountability and demonstrable compliance.

4.4 Confidentiality and human rights

A disclosure may comply with data protection law but still breach confidentiality. Practitioners must identify whether the information was provided or created in circumstances giving rise to an expectation of confidence, then establish consent, statutory authority, a court order, or a sufficiently strong public-interest justification for disclosure.

Any interference with private and family life must be in accordance with law, pursue a legitimate aim and be necessary and proportionate. The record should identify the competing rights and risks where the interference is significant.

4.5 Care Act powers and duties

Sections 6 and 7 support cooperation between the local authority and relevant partners.

Section 42 requires the local authority to make, or cause to be made, whatever enquiries it

considers necessary where the statutory criteria are met. Section 44 provides for Safeguarding Adults Reviews. Section 45 enables a Safeguarding Adults Board to request information needed to enable or assist it to exercise its functions, subject to the statutory conditions and limitations.

Section 45 is not the routine legal basis for all operational sharing. Formal section 45 requests must be authorised through the LSAB Chair or a documented delegate and must identify the SAB function, information required, recipient, deadline, secure route, and any restrictions.

5. Parties, roles, and accountability

5.1 Controller status

Unless a data flow schedule states otherwise, each partner acts as an independent controller for the information it holds and for its decision to disclose, receive and further process that information. Signature of this agreement does not, by itself, create joint controllership or a processor relationship.

Where partners jointly determine purposes and essential means, they must complete a joint-controller arrangement allocating responsibility for transparency, individual rights, security, breaches, retention, complaints, and contact arrangements. Where a partner processes solely on behalf of another controller, an Article 28-compliant contract must be in place before processing begins.

5.2 Required partner contacts

Function	Minimum contact required
Senior accountable owner	Executive lead with authority to commit the organisation.
Safeguarding lead	Operational escalation and practice advice.

Function	Minimum contact required
Data Protection Officer / IG lead	Data protection, rights, complaints, DPIA and breach advice.
Caldicott Guardian, where applicable	Confidentiality and health or care information advice.
Security incident contact	Twenty-four-hour or urgent incident route where available.
FOI contact, where applicable	Freedom of information and publication decisions.
Legal contact	Complex statutory, confidentiality, human-rights, and disclosure advice.

5.3 Accountability of each partner

- Maintain a record of processing activities and the data-flow schedules relevant to this agreement.
- Provide current privacy information and an accessible data protection complaints route.
- Train staff and regularly assure competence.
- Apply role-based access, joiner-mover-leaver controls, and periodic access review.
- Complete DPIAs were required and implement resulting actions.
- Maintain appropriate policy documents for relevant Schedule 1 processing.
- Keep auditable decision, disclosure, correction, and incident records.
- Notify the LSAB Board Manager promptly of changes that materially affect this agreement.

6. Permitted purposes, information, and recipients

6.1 Permitted safeguarding purposes

- Preventing death, serious harm, abuse, or neglect.
- Assessing, referring, planning, conducting, or reviewing a safeguarding enquiry.
- Protecting children, other adults, or the public from identified risk.
- Preventing or detecting crime, supporting investigation or prosecution, or managing risk posed by a suspected perpetrator, were lawful.
- Making a lawful referral to the Disclosure and Barring Service, regulator, commissioner, employer, or professional body.
- Conducting a Safeguarding Adults Review or other statutory learning process.
- Identifying patterns, organisational abuse, repeat concerns, or systemic risk.
- Monitoring equality, effectiveness, and outcomes where identifiable data is necessary and appropriately governed.
- Handling complaints, professional concerns, or governance failures linked to safeguarding.
- Enabling the LSAB to exercise its statutory functions.

6.2 Categories of information

Depending on necessity and proportionality, information may include identifiers and contact details; care and support needs; health and communication needs; family and relationship information; safeguarding concerns and risks; capacity and advocacy information; allegations, incidents, and professional assessments; criminal offence data; service involvement; equality information; images, audio, or video; and actions or outcomes. Information must be limited to what is needed for the defined purpose.

6.3 Recipients and access

Only a person with a legitimate role and need to know may receive or access identifiable information. Meeting attendance, employment by a partner or access to a shared system does not establish a need to know. Circulation lists must be checked before every disclosure, and blanket copying of records or emails must be avoided.

6.4 Routine and systematic sharing

No routine, bulk, matched, repeated or system-to-system sharing may begin until Appendix C is completed and approved by the relevant controllers. The schedule must define purpose, data, frequency, recipients, roles, legal bases, confidentiality basis, security, retention, rights arrangements, DPIA status and owner.

7. Decision-making, consent, capacity, and confidentiality

7.1 Decision test

17. Define the safeguarding purpose and intended outcome.
18. Confirm identity, authority and need to know of the requester and recipient.
19. Identify the information needed and remove irrelevant material.
20. Identify Article 6 and, where relevant, Article 9 or Article 10 / DPA 2018 conditions.
21. Consider confidentiality, human rights, professional duties, and any legal restriction.
22. Consider the person's views, consent, or objection and whether it is safe and appropriate to inform them.
23. Consider capacity for the specific decision and provide practicable support.
24. Balance the risks and benefits of sharing, partly sharing, delaying, or not sharing.
25. Use a secure route and record the decision and disclosure.
26. Review or escalate where risk, disagreement or uncertainty remains.

7.2 Consent and objections

UK GDPR consent should be used only where it is freely given, specific, informed, unambiguous and capable of being withdrawn without detriment. It is often not the appropriate lawful basis for statutory adult safeguarding. A person's agreement, refusal, or objection remains highly relevant to person-led practice and confidentiality even where another data protection basis is used.

Information may be shared without consent where this is lawful, necessary, and proportionate, including to exercise statutory functions, protect the person or others, prevent or detect serious crime, comply with a court order, or pursue an overriding public interest. This is not limited to an immediate emergency. Practitioners should record why the person was not asked, why an objection was overridden, and whether the person was informed afterwards.

7.2A Transparency after sharing without agreement

A person should normally be told what was shared, with whom, why and under what authority, even where their agreement was not required. Information may be delayed or limited only where telling the person would be unsafe, impossible, seriously prejudice the safeguarding or legal purpose, breach another person's rights, or where another lawful restriction applies. The reasons and the information withheld must be recorded. The decision must be reviewed, and the person must be informed later when the reason for delay no longer applies, unless there remains a lawful reason not to do so.

7.3 Mental capacity

Capacity is presumed unless established otherwise and must be assessed for the specific information-sharing decision at the relevant time. All practicable steps must be taken to support the person, including accessible information, communication support, and sufficient time where risk permits.

Where the person lacks capacity, any decision made on their behalf must follow the Mental Capacity Act 2005, including best-interests' principles, the least restrictive option and consideration of wishes, feelings, beliefs, values, and relevant representatives. A valid attorney or deputy may have a relevant role, but safeguarding duties and risks to others must still be considered. Independent advocacy must be arranged where legally required.

7.4 Urgent situations

Where delay may expose a person to death, serious harm or escalating abuse, relevant information should be shared promptly with those able to act. The disclosure must still be limited to what is necessary, use the safest available route and be recorded as soon as practicable. Lack of access to a manager must not prevent necessary emergency action.

7.5 Refusal or delay

A refusal or delay must state the reasons and identify any alternative, narrower or conditional disclosure that could meet the purpose. The requester should escalate through safeguarding and information governance routes. If information is required to enable or assist the SAB to exercise its functions, formal use of section 45 Care Act 2014 may be considered. Refusal decisions may be referred to the DPO, IG lead, Caldicott Guardian, legal adviser or senior safeguarding lead, as appropriate.

8. Operational sharing arrangements

8.1 Request requirements

Requests should use Appendix A unless an emergency makes this impracticable. They must be specific, necessary, time-bound and sent to an authorised contact. A request for an entire record must explain why selective disclosure cannot meet the purpose.

8.2 Decision and disclosure record

The disclosing organisation must complete Appendix B or an equivalent record. The record must identify what was shared or withheld, with whom, under which legal and confidentiality basis, by what method, on what date, with what restrictions and why the decision was necessary and proportionate.

8.3 Secure transfer

- Use an approved encrypted system or secure portal wherever available.
- Confirm the recipient's identity, role and address using a trusted source, not solely the request message.
- Use protective marking and a clear subject line without unnecessary personal data.
- Password-protect files where required and transmit passwords separately.
- Check attachments, recipients, and distribution lists before sending.
- Confirm receipt for high-risk or time-critical information.
- Avoid personal email, unapproved cloud storage, messaging applications, removable media, or consumer AI tools.
- Where an insecure disclosure occurs, contain the risk and report it immediately.

8.4 Accuracy, opinion, and correction

Shared material must distinguish verified fact, allegation, professional opinion, and third-party information. The source and date should be included where relevant. Material errors, misleading omissions, or changed risk information must be communicated to recipients without undue delay, and the correction trail must be retained.

8.5 Meetings and minutes

Invites and papers must be limited to appropriate attendees. The chair must remind participants about purpose, confidentiality, onward sharing, and secure disposal. Minutes

should avoid unnecessary personal data, accurately record decisions, and identify any restricted distribution. Recordings or AI transcription require prior approval under section 11.

8.6 Access to shared systems

Inter-organisational system access requires a written access agreement, role design, authentication controls, audit logging, training, confidentiality requirements, support arrangements, access review and prompt removal on role change or departure. Users must not browse records outside their legitimate relationship or assigned safeguarding function.

9. Transparency and individual rights

9.1 Privacy information

Each controller must provide clear, accessible privacy information covering identity and contact details, purposes, lawful bases, data categories, recipients, retention, rights, complaint routes, international transfers, and relevant automated processing. Information may be delayed or limited only where a lawful exemption applies and the reasons are documented.

9.2 Rights requests

Each controller is responsible for rights requests concerning data under its control unless a joint-controller arrangement allocates tasks differently. Partners must cooperate promptly where records have been shared, corrected, or restricted. No partner should promise that another organisation will withhold or disclose information.

9.3 Complaints

Each organisation must maintain an accessible data protection complaints procedure in accordance with current law. Complaints must be acknowledged within 30 days of receipt. The controller must, without undue delay, take appropriate steps to respond to the complaint, including making appropriate enquiries, keep the individual informed of progress where

necessary, and inform them of the outcome without undue delay. Individuals must also be informed of their right to complain to the Information Commissioner.

9.4 Freedom of information

Public authorities must determine Freedom of Information Act and Environmental Information Regulations requests under their own statutory duties. Personal data, confidentiality, law enforcement, legal professional privilege, and effective conduct exemptions must be considered case by case. Consultation with the information originator may assist but does not transfer the decision or create a veto.

10. Security, incidents, retention, and disposal

10.1 Security controls

- Risk-based technical and organisational measures appropriate to the sensitivity and volume of information.
- Multi-factor authentication where appropriate, encryption at rest and in transit, supported software and secure configuration.
- Role-based access, logging, monitoring, and regular access review.
- Physical security for paper records and devices.
- Supplier due diligence, written contracts, and assurance of subcontractors.
- Business continuity, backup, and tested recovery arrangements.
- Staff confidentiality, training, and sanctions for deliberate misuse.

10.2 Personal data breaches

Staff must report an actual or suspected breach immediately through their organisation's incident route and, where practicable, within 24 hours of awareness. The controller must assess risk, contain the incident, preserve evidence, and determine whether notification to

the ICO is required within 72 hours of awareness and whether affected people must be informed without undue delay because of high risk.

Where more than one partner is affected, the discovering organisation must notify the relevant controller contacts promptly. Each controller remains responsible for its own regulatory assessment unless a written joint-controller arrangement provides otherwise. The LSAB Board Manager should be informed of incidents presenting significant multi-agency safeguarding or reputational risk.

10.3 Retention

Information must be retained only as long as necessary for the purpose, subject to legal, regulatory, inquiry, litigation, and safeguarding holds. Appendix C must identify the retention trigger and period for each routine flow. Each partner must apply its approved schedule and document any justified extension.

The organisation with responsibility for the authoritative or master record must be identified. Duplicates should be minimised. Deletion, restriction, or correction affecting another partner must be communicated where necessary to maintain lawful and accurate records.

10.3A Shared-record retention responsibilities

An originating organisation cannot automatically require an independent receiving controller to delete information where the recipient has its own lawful need or duty to retain it. Equally, receiving information does not justify keeping it indefinitely. Each controller must apply its own approved retention schedule, record any legal or safeguarding hold, identify duplicate copies and document departures from the planned period. Appendix C must state the master-record responsibility and how partners will coordinate review, correction, restriction and disposal.

10.4 Secure disposal

Paper records must be disposed of through an approved confidential waste or secure-destruction process appropriate to the organisation's information classification and the sensitivity of the information. Electronic data must be securely erased in accordance with approved technical standards, taking account of backups, archives, legal holds, and supplier systems. Disposal should be auditable for high-risk records.

11. Artificial intelligence and automated processing

11.1 General rule

Personal data must not be entered into, uploaded to, or processed by an AI system unless the relevant controller has expressly approved the system and use case. Approval must cover purpose, lawful basis, confidentiality, DPIA, security, procurement, supplier terms, transparency, equality, human oversight, retention, deletion, and international transfers.

11.2 Minimum controls

- Maintain a register of approved AI systems, use cases, owners, suppliers, and review dates.
- Prohibit use of consumer or personal AI accounts for safeguarding information.
- Confirm whether prompts, recordings or outputs are stored, accessed by suppliers, or used to train models.
- Complete supplier and subcontractor due diligence, including hosting location and international transfer safeguards.
- Validate accuracy and bias before use and monitor performance throughout the lifecycle.
- Clearly mark AI-generated transcripts, summaries or recommendations and retain the source where necessary.
- Require a competent human to review material outputs before they influence assessment, recording, referral, or action.

- Provide understandable information to affected people where appropriate.
- Enable correction, challenge, and human intervention.
- Suspend use where material error, bias, security weakness, or unexpected harm is identified.

11.2A Organisational AI governance

Every AI use must comply with the approving controller's AI policy, acceptable-use rules, information-classification scheme, records-management policy, procurement controls and sector requirements. Approval under this agreement does not replace organisational approval. The controller must name the senior owner who may approve, pause or stop the use case and must keep evidence of the decision.

11.3 Automated decisions

As an LSAB governance requirement, solely automated decision-making producing legal or similarly significant effects must not be used in adult safeguarding unless the processing is lawful, has been expressly approved through the relevant organisation's governance arrangements, and all applicable statutory safeguards have been implemented. Individuals must be provided with the information and safeguards required by law, including appropriate opportunities to make representations, challenge a significant decision and obtain human intervention. Safeguarding judgements, capacity decisions and decisions materially affecting protection or access to support must retain meaningful and effective human oversight.

11.4 AI-assisted transcription

Recording or transcription of meetings requires a defined purpose, approved tool, lawful and confidentiality basis, participant information, secure storage, access controls, retention period, and human verification. The official record must be checked against the meeting and corrected before reliance. Raw recordings and transcripts must not be retained by default beyond the approved purpose.

12. Assurance, escalation, review, and termination

12.1 Training and assurance

Partners must provide role-appropriate induction and refresher training covering safeguarding, lawful bases, confidentiality, capacity, secure transfer, incident reporting, rights, AI, and use of the appendices. The LSAB Executive Group will receive annual assurance on implementation.

Assurance measure	Minimum evidence
Training	Completion rates and targeted action for gaps.
Decision quality	Sample audit of sharing and non-sharing decisions.
Security	Access reviews, incidents, near misses and remedial action.
Timeliness	Delays or refusals that affected safeguarding outcomes.
DPIAs	New, reviewed, and overdue assessments.
Rights and complaints	Volumes, themes, outcomes, and learning.
AI	Approved systems, use cases, incidents, reviews, and suspensions.
Learning	Actions arising from SARs, audits, complaints, and regulatory guidance.

12.2 Escalation and dispute resolution

27. Practitioner-to-practitioner clarification and consideration of a narrower disclosure.
28. Escalation to operational safeguarding managers.

29. Review by DPO / IG lead, Caldicott Guardian or legal adviser as appropriate.
30. Senior accountable owner discussion between organisations.
31. Referral to the LSAB Chair where a SAB function or section 45 request is engaged.
32. Recording of unresolved disagreement, risk management, and any decision to notify a regulator or statutory body.

12.2A Managing urgent disagreement

Where partners disagree, they must first consider whether a narrower, redacted, time-limited or conditional disclosure can meet the safeguarding purpose. Escalation must be immediate where delay may expose a person to serious harm, and otherwise within locally agreed timescales recorded in the partner contact schedule. The senior person making any interim decision must be named. Disagreement must not be used to justify unrestricted sharing or avoidable delay. The final decision, reasons, risk controls, advice obtained and learning must be recorded and communicated to the relevant partners.

12.3 Review

The LSAB Board Manager will coordinate review every two years and sooner where there is a material change in law, ICO guidance, statutory guidance, partner structure, technology, data flow, risk, serious incident, or Safeguarding Adults Review finding. Changes must be version controlled and communicated to all signatories.

12.4 Suspension, withdrawal, and termination

A partner may suspend a specific data flow where serious legal, security or safeguarding concerns arise, but must take proportionate steps to avoid creating additional risk. Withdrawal from the agreement does not remove duties concerning information already received, including confidentiality, retention, correction, breach management, and secure disposal.

13. Sources and supporting standards

- ICO Data Sharing Code of Practice
- ICO: Data (Use and Access) Act 2025
- GOV.UK: Care and Support Statutory Guidance
- GOV.UK: Data (Use and Access) Act 2025 changes
- GOV.UK: Artificial Intelligence Playbook for the UK Government
- GOV.UK: Data and AI Ethics Framework
- NHS England: Information sharing in social care
- SCIE: Safeguarding adults and sharing information
- UK Caldicott Guardian Council: Common law duty of confidentiality
- Legislation.gov.uk: Data Protection Act 2018
- Legislation.gov.uk: Care Act 2014

The above guidance may change. Partners must use the current published version and obtain specialist advice where interpretation is uncertain.

Appendix A: Information sharing request form

Use for non-emergency requests. In an emergency, provide the essential information by the safest available route and complete the record retrospectively as soon as practicable.

Field	Response
Request reference	
Requesting organisation	
Requester name, role, and verified contact details	
Receiving organisation / team	
Date and time of request	
Date and time information required	
Safeguarding purpose and expected outcome	
Specific information requested and relevant date range	
Why each item is necessary and proportionate	
People to whom the information relates	

Field	Response
Known wishes, consent, or objections	
Risk if the person is informed of the request	
Proposed Article 6 lawful basis	
Proposed Article 9 condition, if applicable	
Proposed Article 10 / DPA 2018 condition, if applicable	
Statutory power, duty, or court order	
Confidentiality justification	
Intended recipients and onward sharing	
Requested transfer method	
Retention or deletion requirement	
Requester signature / electronic authorisation and date	

Appendix B: Information sharing decision and disclosure record

Field	Decision record
Request / case reference	
Holding organisation	
Decision-maker name, role, and authority	
Date and time assessed	
Purpose and expected safeguarding benefit	
Requester identity and authority verified	Yes / No / Not applicable. Evidence:
Need to know established	Yes / No. Rationale:
Information considered	
Information to be disclosed, withheld or redacted	
Article 6 lawful basis	
Article 9 condition and Schedule 1 condition, if applicable	

Field	Decision record
Article 10 / DPA 2018 condition and appropriate policy document, if applicable	
Statutory power, duty, or court order	
Confidentiality basis	Consent / statutory authority / court order / overriding public interest / other:
Person informed or consulted	Yes / No / Not safe or practicable. Reasons:
Views, consent, or objection	
Capacity for this specific decision	Has capacity / lacks capacity / not in doubt / not relevant. Evidence and support provided:
Best-interests' considerations, if applicable	
Human rights, equality, and risk considerations	
Necessity, proportionality, and data minimisation	
Risk of sharing	
Risk of not sharing or delay	

Field	Decision record
Decision	Share / partly share / defer / refuse / escalate
Reasons for decision	
Recipient name, organisation, role, and verified address	
Transfer method and protective marking	
Date and time sent	
Receipt confirmed	Yes / No / Not required
Onward sharing, use or retention restrictions	
Review / follow-up date	
Corrections, updates, or withdrawal communicated	
Escalation or advice obtained	
Decision-maker signature / electronic authorisation	
Caldicott considerations	Purpose justified / necessary / minimum necessary / need to know / responsibilities / law / duty to share / transparency:

Field	Decision record
Public-interest balancing test	Harm, seriousness, likelihood, rights, alternatives, minimum disclosure and reasons:
Professional confidentiality duties	Applicable code or duty and advice obtained:
Delayed transparency review	Reason, review date, outcome and date person informed:
Partner consultation for rights or disclosure	Organisation consulted, advice, decision and reasons:
Data quality status	Fact / allegation / opinion / intelligence / disputed / corrected:

Appendix C: Data flow and legal basis schedule

A separate schedule should be completed for each routine, repeated, bulk, matched, shared-system or otherwise systematic data flow. Attach diagrams or technical specifications where helpful.

Field	Approved arrangement
Schedule reference and version	
Business owner and review date	
Purpose and measurable benefit	
Data subjects	
Data categories and fields	
Special category data	
Criminal offence data	
Source controller(s)	
Recipient controller(s)	
Controller relationship	Independent / joint / controller-processor
Processor and subcontractors	
Frequency / trigger / volume	
Article 6 basis	
Article 9 and Schedule 1 condition	

Field	Approved arrangement
Article 10 and Schedule 1 condition	
Statutory power or duty	
Confidentiality basis	
DPIA reference and residual risk	
Privacy information arrangements	
Individual rights and complaints responsibilities	
Security, access, and transfer controls	
International transfer and safeguard	
Accuracy and correction process	
Master record owner	
Retention trigger and period	
Deletion / return arrangements	
Breach notification contacts and timescales	
Audit and assurance measures	
Approvals	

Field	Approved arrangement
Originating organisation	
Authoritative/master-record custodian	
Supplementary agreements required	DPIA / joint-controller arrangement / processor contract / system access / technical schedule / transfer assessment
Rights-request lead and consultation timescale	
Third-party information process	
Exemption decision and escalation route	
Dispute escalation timescales and interim decision-maker	
Caldicott Guardian review, where relevant	

Appendix D: Practitioner decision pathway

33. Is a living person identifiable? If not, confirm that anonymisation is effective. If yes or uncertain, continue.
34. What safeguarding purpose and outcome require the information?
35. Who needs the information, and has their identity, authority and role been verified?
36. What is the minimum necessary information?
37. Which Article 6 lawful basis applies?
38. Does the information include special category data? If yes, identify Article 9 and DPA 2018 conditions.
39. Does it include criminal offence data? If yes, identify Article 10 authority and DPA 2018 condition.
40. Is the information confidential? Identify consent, statutory authority, court order or overriding public interest.
41. Has the person been informed and supported to express views? If not, record why.
42. Is capacity in doubt for this specific decision? If yes, support, assess and apply the Mental Capacity Act.
43. What are the risks and benefits of sharing, partly sharing, delaying, or not sharing?
44. Can the information be shared securely and accurately now?
45. Record the decision, disclosure, recipient, method, restrictions, and review actions.
46. Escalate unresolved risk or disagreement without avoidable delay.

If immediate action is required

Share the minimum necessary information with the person or service able to act, using the safest available method. Record and escalate as soon as practicable.

Appendix E: Partner signatories

Partner organisation	Authorised signatory	Signature	Date
Cheshire West and Chester Council			Sep-26
Cheshire Constabulary			Sep-26
NHS Cheshire and Merseyside Integrated Care Board			Sep-26
Age UK Cheshire			Sep-26
Cheshire Fire and Rescue Service			Sep-26
Cheshire and Wirral Partnership NHS Foundation Trust			Sep-26
Countess of Chester Hospital NHS Foundation Trust			Sep-26
Disability Positive			Sep-26
Healthwatch Cheshire West			Sep-26
Mid Cheshire Hospitals NHS Foundation Trust			Sep-26
Probation Service - Cheshire			Sep-26

Partner organisation	Authorised signatory	Signature	Date
North West Ambulance Service NHS Trust			Sep-26
Weaver Vale Housing Trust			Sep-26
VoiceAbility Cheshire			Sep-26

By signing, each organisation confirms that it has authority to enter the agreement, has identified its accountable contacts, will complete relevant data-flow schedules, and will comply with the controls and escalation arrangements set out above.