Stockport Safeguarding Children Partnership & Stockport Safeguarding Adult Partnership

Information Sharing and Retention Agreement

Stockport Safeguarding Children Partnership & Stockport Safeguarding Adult Partnership
Information Sharing and Retention Agreement

Contents

Version History

Date Issued	Version	Status	Reason for change
10/03/2021	2	Draft	Developed SSAB document into shared ISA & Retention agreement
23/02/2022	3	Draft	Appendices updated and content regarding DIPA and retention schedules updated
14/07/2022	4	Final	Approved at Joint Safeguarding Partnership Executive Board

Purpose & Scope

This document outlines the commitment from the Stockport Safeguarding Adult Board (SSAB) and Safeguarding Children Partnership (SSCP) to comply with law and regulations in relation to Data Protection Legislation. This is to ensure that the Partnerships endeavour to meet their statutory duties to seek assurance and apply scrutiny with a proportionate and secure approach to data collection, use and retention.

The following pages will outline the approach taken, the storage facilities utilised and the retention policy in place.

This agreement provides a framework for the sharing of data and information relating to the protection of adult at risks from abuse and the safeguarding of children expected by strategic safeguarding partnerships. It is in line with The Social Care Institute for Excellence's Adult Safeguarding; Sharing Information Guide[1] and expectations as outlined in Working Together 2018[2]

This agreement will cover all data that is held or controlled by the Safeguarding Partnerships. This includes physical hard copy documents, contracts and letters and electronic data such as emails, electronic documents, and audio recordings. There are legal and regulatory requirements regarding the retention of data for day-to-day operational needs or specific purposes.

This agreement relates purely to data and information collected on behalf of the statutory safeguarding partnerships. Each individual partner will be responsible for their own internal data processing and retention in line with their own purpose and function. All references to data and information within this document refers to that requested, processed and stored to discharge the statutory duties of the multi-agency safeguarding partnerships. This will include work undertaken by the Safeguarding partnerships team and any contractors engaged with such as independent authors.

In seeking access to data and information the Safeguarding partnerships in Stockport will endeavour to respect the rights of privacy when undertaking their statutory duties.

Freedom Of Information requests

The Safeguarding Partnerships are not public authorities for the purposes of the Freedom of Information Act 2000 (FOIA) and are therefore exempt from the duty to provide access to information held by them.

Section 3 of the FOIA provides that:

(2) For the purposes of this Act, information is held by a public authority if—
(a) it is held by the authority, otherwise than on behalf of another person, or
(b) it is held by another person on behalf of the authority.

A FOI request may be made directly to partner agencies of the Safeguarding Partnerships. The parties agree that where a SSCP or SSAB partner which is deemed to be a public authority under the FOI holds information for its own purposes, then it does so otherwise than on behalf of another person and the information held

[1] https://www.scie.org.uk/safeguarding/adults/practice/sharing-information

[2] https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

will be subject to the FOI. However, partners in possession of SSCP and SSAB minutes, documents, reports etc. are holding this information on behalf of 'another person' (either SSCP and SSAB) and it is therefore not liable to disclosure under a FOI request. In all instances all partners agree no records of meetings will be produced or shared without the express permission of the Chair.

Legal Responsibility to Share Information & Good Practice Guidelines

Information sharing is related to a number of different pieces of legislation and good practice guidance. These can be viewed in more detail in Appendix 1. This agreement has been developed in line with the core data protection legislation and guidance and the requirements placed upon the partnerships by other statutory frameworks as outlined below.

For the SSCP Working Together 2018 outlines the statutory duties they must discharge and in relation to information sharing states:

"Safeguarding partners may require any person or organisation or agency to provide them, any relevant agency for the area, a reviewer or another person or organisation or agency, with specified information. This must be information which enables and assists the safeguarding partners to perform their functions to safeguard and promote the welfare of children in their area, including as related to local and national child safeguarding practice reviews. The person or organisation to whom a request is made must comply with such a request and if they do not do so, the safeguarding partners may take legal action against them." p79-80

The Safeguarding Adult Board operates within the framework of the Care Act Guidance[3] which states:

"An SAB may request a person to supply information to it or to another person. The person who receives the request must provide the information to the SAB if:

- the request is made in order to enable or assist the SAB to do its job
- the request is made of a person who is likely to have relevant information and then either:
    - the information requested relates to the person to whom the request is made and their functions or activities
    - the information requested has already been supplied to another person subject to an SAB request for information" section 14.186

The SSCP and SSAB must ensure to comply with basic Information Commissioner's office guidance when seeking information as outlined above as laid out in the statutory code of practice prepared under section 121 of the Data Protection Act 2018[4] (DPA 2018). All activity will be undertaken inline with the core principles, set out in Article 5 of the UK General Data Protection Regulation (UK GDPR):

- Data must be processed ***Lawfully, fairly and transparently***
- It should be collected for specific & legitimate ***purpose***
- The process should aim to collect that which is ***adequate & relevant*** to need

[3] https://www.gov.uk/government/publications/care-act-statutory-guidance/care-and-support-statutory-guidance#safeguarding-1
[4] https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/about-this-code/

- ***Accurate & kept up to date***
- Kept for no longer than is ***necessary***
- Kept in a way that offers appropriate ***security and confidentiality***
- The controller should be able to demonstrate ***accountability*** for compliance with these principles

The following pages will outline the Partnerships approach to requesting, processing and retaining data to discharge their statutory duties.

Exemptions

It is not always appropriate/possible to identify a lawful basis for sharing information. Schedules 2 – 4 of The Data Protection Act 2018[5] set out a number of exemptions which should be considered should this be the case. Exemptions should not routinely be relied upon or applied in a blanket fashion. Each exemption should be considered on a case-by-case basis. As the work of the Safeguarding Partnerships may fall into these areas at times then it may be that some activity calls upon exemptions to progress. For example, there are exemptions when sharing relates to the prevention or detection of crimes. Where this may arise, the partnerships will document that this is the case.

Parties to the Agreement

All parties signed up to this agreement are committed to ensure that all staff who are involved in Safeguarding Partnership activity understand and comply with their responsibilities to share information in accordance with this Agreement and UK GDPR expectations.

Formal adoption of this protocol is the responsibility of the Chief Executives/ Head of each Organisation and where appropriate Caldicott Guardians.

SSAB & SSCP will be responsible for the overall approval, maintenance and review of this protocol and will ensure dissemination of this protocol and monitor the implementation and compliance of this framework within their support team and wider partner engagement.

All parties have a responsibility to ensure that all members of staff are aware of this protocol and the framework for sharing personal and sensitive information. All parties should attend appropriate Information Governance Training within their own organisations, and raise awareness, and ensure that their staff attend the appropriate training.

All parties have a duty of confidentiality and to ensure that individual rights in relation to the disclosure and use of personal information are understood.

The specific agencies involved in this agreement are asked to sign in **Appendix 2** with details of their Data Protection Officer (DPO) and any other relevant employee with data sharing responsibilities.

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

Where additional agencies need to be included but are not specifically referenced in this document, they will be asked to sign the document in **Appendix 3** to indicate their acceptance of these arrangements and agreement to abide by the principles contained within. These relevant agencies may either agree to sign up to the arrangements as a permanent member or make a temporary arrangement if the information sharing is to be time limited. For example, Independent Authors of Safeguarding Adult Reviews may be asked to sign the document for the period of time they are engaged in report writing.

The data collected for statutory purposes is ultimately controlled by the Partnership itself, via its support team, as each agency owns its own data so they are collectively responsible for it being processed for partnership purposes. The individual responsible for the collection and processing of the data (Data Processing officer) for the Partnerships is the Safeguarding Partnership Lead.

If you wish to contact the Safeguarding Partnerships please call 0161 474 5657 or email lsb@stockport.gov.uk

Information to be shared

The SSCP and SSAB will require data, intelligence and at times personal information in order to discharge their statutory functions. The table below offers an overview of the most common information required and the lawful basis for sharing, more information regarding lawful basis can be found in Appendix 4.

Type of Information	Nature	Purpose of Collection	Lawful Basis for Sharing
Statistical Information in relation to Children in receipt of Universal Services, Children in Need, Children subject to Child Protection Plans and Children who are looked after. Adults at risk under S42 and subject to safeguarding processes.	Figures, Commentary, Case studies	Section 11 Compliance audits Multi-agency audits of practice to assess the effectiveness of multi-agency working locally	The lawful basis for this collection of personal data is statutory duties as identified in Working Together 2018 and the Children and Social Work Act 2017 and the Care Act Statutory Guidance. In essence the statutory guidance places expectations on the partnerships to collect information to undertake checks on practice either as learning reviews or
Performance data in relation to the above	Figures, Commentary	For the Partnerships to seek assurance about safeguarding activity and its impact on the outcomes for children, young people, adults and families	

Agency reflection records such as Individual Management Review reports, Agency Contact reports (RR, CSPR & SAR processes)	Name DOB Address Occupation Social circumstances (may include ethnicity) Details of respective family members Health records Education records Local Authority records Police records Any Specialist service provision Any outcomes for the person from the interventions Any feedback the person has given services Information relating to the person's alleged or proven, past or present criminal offences The person's movements, habits, conduct or practises.	Multi-agency learning reviews to capture system issues or good practice Child Safeguarding Practice Reviews and Rapid Reviews where a child or young person has died or experienced abuse and or neglect that has resulted in serious harm Adult SAR screening or learning processes where an adult with care and support needs has died or experienced abuse and or neglect that has resulted in serious harm	through other processes, such as audit, that allow them to apply scrutiny to compliance with Section 11 of the Children's Act 2006. Section 11 of this Act tells agencies what they must have in place to meet their safeguarding responsibilities, such as staff training and safeguarding leads. Alongside this the Care Act statutory guidance places requirements that agencies are sufficiently equipping staff to recognise and respond to safeguarding concerns relating to adults at risk. Therefore, this collection of data is undertaken as a Legal Obligation or Public Task. A Public Task is something public bodies have the power to do and a Legal Obligation is a task that the public body have a duty to, or must do, as it is set out in law. It refers to activity that is set out in law as activity in the public interest. For example, if a child dies then a learning review can
Practice Self-assessment audit tools	Policies, Procedures, Commentary, Figures, Service User feedback	Section 11 Compliance audits Multi-agency audits of practice to assess the effectiveness of multi-agency working locally	

			identify how the safeguarding system did not work and seek to make changes to reduce the chances of such a death occurring again.

It should be noted that some of the information collected will likely contain special category data. This is defined as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

Processing of this data is only allowed if the purpose meets specific conditions. For the purposes of the Safeguarding Partnerships the purpose of this collection would pertain to "reasons of substantial public interest" and the statutory duty to conduct scrutiny and seek assurance as laid out in statutory guidance mentioned above. Similarly, Criminal Offence data requires specific conditions to be met for processing. In this instance the conditions from Schedule 1 of the DPA 2018 that apply are safeguarding children and individuals at risk and statutory or government purposes.

Where this information is required there may be a need for a Data Protection Impact Assessment (DPIA). The SSCP and SSAB team will ensure that DPIAs have been completed on behalf of the partnership for the 3 core data collection activities; Reviews, Audits and Data Dashboards. Appropriate advice will be sought where relevant for these activities.

Right to Access & Objection

The UK GDPR gives people the right to apply to an organisation that holds personal information about them for access to that information. The exercise of this right is referred to as a subject access request. People may exercise this right on their own behalf or through a representative. Where people do not have the mental capacity to make a request on their own behalf, because they are too young or for some other reason, their parent or person with Power of Attorney may make the request on their behalf.

The right of subject access applies to all personal information held by an organisation about that data subject regardless of whether or not that organisation is the "owner" or "source" of the information. The

information must be disclosed to the data subject unless one of the exemptions in the Data Protection Act applies. It may be appropriate for the organisation that has received the subject access request to consult with the source of the information they hold to discuss whether the information is subject to an exemption.

Any information shared with the Partnerships is for a specific purpose of scrutiny or review. Therefore, does not constitute a case record. Individuals will have the right to query and object to the information shared with the Partnerships but issues of accuracy in their personal records will relate to individual members internal processes. Therefore, these concern's will be directed to the individual relevant partner. For example, if an adult at risk identifies that information reported in a SAR is factually incorrect, they will need to speak to the individual agency that holds that record for rectification. The Partnership will amend the retained learning document produced from that information but the original record will need to be discussed with the partner agency over which the Partnership itself has no authority.

All partner organisations that are party to this protocol will put in place procedures for handling requests for personal information.

All Subject Access Requests must be made to the relevant data controller and the subsequent actions taken must be fully recorded within the organisations system. Information obtained from a partner organisation without the prior consent of the data subject cannot be disclosed to that individual without the agreement of the originating organisation. This does not prevent the individual making a separate Subject Access Request to the originating partner organisation.

Agencies must make sure that data will be received by the requester no later than one calendar month from receipt of a valid request.

Basic Information Governance Compliance Requirements For Members

In signing this agreement partners and relevant agencies are confirming that the following is in place:

- considered which datasets they can share, to prevent irrelevant or excessive information being disclosed;
- ensure that the data is accurate;
- record data in the same format, abiding by open standards when applicable;
- accept the rules for the retention and deletion of shared data items;
- have common technical and organisational security arrangements e.g. for safe transmission of the data and procedures for dealing with any breach of the agreement in a timely manner;
- ensure their staff are trained and aware of their responsibilities for any shared data;
- have procedures for dealing with access requests, complaints or queries from members of the public;

They also agree to review this agreement on an annual basis or sooner should a complaint or breach suggest the need for further measures.

Secure Storage and Sharing of Information

The SSCP and SSAB team are hosted by Stockport Metropolitan Borough Council (SMBC) who provide all employment services including office space and technology. This includes access to secure storage for partnership documents and information. Moving forward SMBC will be utilising SharePoint as a secure website-based storage system for all electronic documents. All information shared electronically will be

retained within this secure storage facility. The management and coordination of all electronic information is restricted to those employed as part of the Stockport Safeguarding Partnerships Business Unit. Information gathered and shared as part of Partnership safeguarding activity will be reviewed by the relevant Safeguarding Partnership Business Manager in advance. For any physical documents provided the team will ensure these are retained on Council property within the Civic Complex. This will be in a restricted access office space that requires official identification and electronic access permissions to gain entry.

The Partnership will ensure safe sharing of information through the following means:

1. Transfer of Information Verbally – the identity of persons involved will be clearly confirmed and in a secure private space so it cannot be overheard by those not part of the processing work.
2. Transfer of Information by Post (Internal or External) - Printed information, or other media, containing personal information will only be sent by post marked "Personal & Confidential", recorded or special delivery methods, and the addressee is informed of when and how the item was sent. This would be limited and would occur as an execption, with secure electronic information sharing prioritised wherever possible.
3. Transfer of Information by Email - Email is not always a secure method of sending personal sensitive information unless encryption is used. All documents sent this way will be encrypted & password protected. Passwords will be sent via separate communication. Personally identifiable information will not be included in the body of emails, with reference numbers, pseudonyms or other initials instead. Preferably this form of communication will be used with known secure email such as; gsi.gov.uk, gsx.gov.uk, gse.gov.uk, scn.gov.uk, gsisup.co.uk, pnn.gov.uk, pnn.polive.uk, cjsm.net, cjsm.gov.uk, nhs.net
4. Transfer through SharePoint sharing – This is a secure site, and is the Safeguarding Partnerships' preferred method of communication. SharePoint allows documents to be held and only accessed by individuals given access permissions. It is hosted by SMBC and provides a forum in which documents can be shared across relevant partners without the need to transfer data.

For the avoidance of doubt the Partnerships will not process shared personal data (including disclosing, transferring or storing) outside the UK.

Retention & Destruction of Records

The UK GDPR dictates that data must not be kept for longer than it is needed and therefore it is necessary to identify retention periods for the personal data which is processed. The Safeguarding partnership Team will retain oversight of relevant retention and destruction periods, for both publicly available information (e.g. Safeguarding Adult Review reports) and restricted documents (e.g. audit returns or IMRs). **Appendix 5** contains the current retention and destruction schedule based on the IAR.

This schedule relates to all hard copy and electronic records. Before destruction the retention period will be checked against any updates to guidance on management of records. This can be found at https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/

This guidance pertains to records held by health and social care. In the main the Partnerships will not hold original records, instead they will access information from these records to produce final products for publication. For example, we request Individual Management Reviews (IMR) to be able to compile a

learning review report. The report is the property of the Partnership and will be retained. The IMR is a collection of data from an original record and so remains the property of the agency that provides it. It will be destroyed from partnership records once the purpose for which it was requested is complete. Retention periods are outlined in Appendix 5 and take into consideration issues such as subject access requests (SAR) and complaints that may be triggered at the point of publication. Where ongoing SAR or complaints exist the retention period may be subject to extension.

Once destruction is determined as appropriate the team will ensure that both hard copy and electronic information is destroyed safely. For example, through the use of confidential waste bins and through electronic destruction that prevents recovery.

By signing this agreement partners are confirming their agreement with the proposed schedules.

Breach Reporting

Where the standards outlined in this agreement are not met and it is felt a "breach" has occurred the Partnerships Team will follow the SMBC breach policy. This entails a report to a line manager and review of the incident by information governance to identify the appropriate next steps.

Any such breaches of partners information will be notified to them directly without undue delay and within one working day and with confirmation of the resolution steps taken e.g. confirmation the 3rd party has deleted the information shared. A log of these breaches will be maintained by the team to ensure that the partnerships are aware of such activity moving forward.

Review and Audit

This protocol will be reviewed by the Partner Organisations annually.

The review is to be undertaken jointly by officer agreed by the Partner Organisations unless agreed by the Partner Organisations for a single Partner Organisation to undertake the review. This work will be co-ordinated by the Safeguarding Partnerships Team.

Partner Organisations may audit compliance with this protocol. Partner Organisations agree to assist other Partner Organisations during the audit process as long as reasonable notice is given in writing detailing the scope of the audit process and they do not object.

Advice and Guidance

The General Data Protection Regulation can be accessed via the Information Commissioner's website at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

The NHS Confidentiality Code of Practice is available at https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

Caldicott requirements are available at www.dh.gov.uk

CQC website www.cqc.org.uk

Legislation website www.bailii.org and http://services.parliament.uk/bills
SCIE's Adult safeguarding: sharing information guide is available at www.scie.org.uk

Appendix 1 – Legal Framework for Information Sharing

Care Act 2014

Under the Care Act 2014 a local authority must:

a) Set up a safeguarding board; the board will share strategic information to improve local safeguarding practice

b) Cooperate with each of its relevant partners; each relevant partner must also cooperate with the local authority.

Clause 45 of the Care Act focuses on 'supply of information'. This relates to the responsibilities of others to comply with requests for information from the safeguarding adults board.

Statutory guidance to the care Act emphasises the need to share information about safeguarding concerns at an early stage and information sharing agreements or protocols should be in place.

Designated adult safeguarding managers in the local authority and the partner agencies 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.

The Common Law Duty of Confidentiality

Common law requires that information **may not be lawfully** disclosed when given in certain circumstances of confidentiality. Disclosure of confidential information **can be justified** if:

- The individual to whom the duty of confidentiality is owed, provides informed consents to the disclosure,
- There is an overriding public interest in disclosure,
- Disclosure is required by a court or other obligation,
- If the individual who is owed confidentiality does not have the mental capacity to consent then disclosure can be made providing a capacity assessment has been undertaken in line with the Mental Capacity Act.

UK GDPR and The Data Protection Act 2018

These provide the main legislative framework for confidentiality and information sharing guidance. Article 5 of The General Data Protection Regulation stipulates seven principles which must be followed when personal information is "processed" by organisations. These are listed below: (see Appendix 1 for further detail)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation

- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

The Act also stipulates the conditions (i.e. the lawful basis) under which information may be shared or processed. There are 6 Lawful Bases detailed in Article 6 of UK GDPR and an organisation must ensure they identify which of these they intend to base their sharing/processing on.

These are listed below: (See Appendix 3 for further detail)

- Consent
- Contract
- Legal Obligation
- Vital Interests
- Public Task
- Legitimate Interests

Example – As a council, if you are carrying out a task which forms part of your official function and the task has a clear basis in law, this would come under Public Task.

The Caldicott Principles (Revised December 2020)

Principle 1: Justify the purpose(s) for using confidential information *Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.*

Principle 2: Use confidential information only when it is necessary *Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.*

Principle 3: Use the minimum necessary confidential information *Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.*

Principle 4: Access to confidential information should be on a strict need-to-know basis *Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.*

Principle 5: Everyone with access to confidential information should be aware of their responsibilities *Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.*

Principle 6: Comply with the law *Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.*

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality *Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.*

Principle 8: Inform patients and service users about how their confidential information is used *A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.*

Appendix 2 – Partner Agency Data Protection Leads

Agency	Named DPO/DP Lead	DPA Role	Contact details
Age UK Stockport			
Stockport Metropolitan Borough Council	Karen Lane	Data Protection Officer	Dpa.officer@stockport.gov.uk
Greater Manchester Fire and Rescue Service			
Greater Manchester Police			
National Probation Service			
North West Ambulance Service			
Pennine Care NHS Foundation Trust			
Stockport Clinical Commissioning Group	Karen Lane	Data Protection Officer	Dpa.officer@stockport.gov.uk
Stockport and Trafford Probation Services			
Stockport NHS Foundation Trust			
Stockport Healthwatch			
Stockport Homes			

Appendix 3 – Additional Relevant Agencies Agreement

Safeguarding Adults in Stockport

Safeguarding Children in Stockport

The following document is to be signed by any relevant agency requested to participate in either SSCP or SSAB statutory duties that requires the sharing of personal and/or sensitive data. This agreement is between the Strategic Partnership and the below referenced relevant agency. It signifies agreement to abide by the processing, use, storage and retention requirements as outlined in the Partnerships Safeguarding Information Sharing Agreement.

It should be used when a relevant agency has not already signed up to the aforementioned agreement as they are infrequently subject to information requests from the partnerships.

DATE	
NAME	
TITLE	
DPO ROLE	
SIGNATURE	
COMMITMENT	The above signed commitment to follow the expectations as laid out in the SSCP and SSAB Information Sharing Agreement & Retention Policy. By signing this document, they also affirm that as an individual agency they are abiding by DPA and UK GDPR expectations and regulations.
TIMEFRAME	*(IF THIS AGREEMENT IS TEMPORARY PLEASE NOTE WITHIN THIS SECTION THE TIME PERIOD THIS WILL BE IN PLACE)*

Appendix 4 – Lawful Bases for sharing/processing personal data

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Appendix 5 – Retention & Destruction Schedule

Function	Activity	Description	Retention Action & Period	Notes
TBD	Safeguarding Adult Review (SAR) and associated activity	All documentation relating to Safeguarding Adult Reviews (SAR) & SAR referral information, Chronolator and IMRs, Author information, Meetings and Events, Email Records, Terms of Reference, Panel Membership, Medical Info, Family details, GCSX emails	Content of file to be deleted **1 year** after publication of the review with the exception of the following: • Original and PDF versions of the report • Original and PDF versions of executive • summary • Original and PDF version of learning • bulletin The three items listed above will be retained for a period of **6 years** after publication	
	Child Safeguarding Practice Review (CSPR) & Rapid Review (RR) and associated activity	All documentation relating to CSPR or RR. Referral forms, agency contact forms, emails, chronologies, meeting minutes, panel details, TOR	Content of file to be deleted 1 year after publication of the review with the exception of the following: • Original and PDF versions of the report • Original and PDF versions of executive • summary • Original and PDF version of learning • bulletin The three items listed above will be retained for a period of 15 years after publication	
	Meetings	All documentation relating to meetings held as part of the SSAB and SSCP governance structure including Executive and Board and a number of sub-groups. Minutes Agendas MOUs	All records to be deleted **5 years** subsequent to the date of the meeting, with the exception of ToRs and MoUs which will be deleted **2 years** after publication of an updated version.	

		ToRs Supportive documents		
	Non statutory / published learning	All documentation relating to the review: referral information, Chronolator and IMRs, Author information, Meetings and Events, Email Records, Terms of Reference, Panel Membership, Medical Info, Family details,	Content of file to be deleted **1 year** after publication of the review with the exception of the following: • Original and PDF versions of the report • Original and PDF versions of executive • summary • Original and PDF version of learning • bulletin The three items listed above will be retained for a period of **10 years** after publication	
	Consultancy Contracts	Consultancy contracts created for: SAR/CSPR Authors Chair of the Partnership	Content of file to be deleted **3 year** after end of contract	
	Tri-X	Contractual agreements with external supplier	Content of file to be deleted **3 years** after end of contract	
	Policy & Procedures	Copies of statutorily required polices, procedures, protocols, flowcharts and templates.	All copies and supporting documentation of polices, procedures, protocols, flowcharts or templates are to be deleted **5 year** after publication of superseding versions.	
	Audits	Information collected as part of an audit - Collated data created as part an audit.	All records, collected information and collated data to be deleted **2 years** after audit is completed	
	Team Information	Information pertaining to staff supervision: Appraisals Supervision	All information pertaining to employees or consultants should be retained in accordance with SMBC policy	

Appendix 6 – Signatories to this agreement

Agency	Lead Officer	Position
Age UK Stockport		
Stockport Metropolitan Borough Council		
Greater Manchester Fire and Rescue Service		
Greater Manchester Police		
National Probation Service		
North West Ambulance Service		
Pennine Care NHS Foundation Trust		
Stockport Clinical Commissioning Group		
Stockport and Trafford Probation Services		
Stockport NHS Foundation Trust		
Stockport Healthwatch		
Stockport Homes		