Information Sharing Protocol
August 2019

Purpose

All persons have the right to live their lives free from violence and abuse. This right is underpinned by the duty on public agencies under the Human Rights Act (1998) to intervene proportionately to protect the rights of citizens.

These rights include:

- Article 2: “The right to life”;
- Article 3: “Freedom from torture” (including humiliating and degrading treatment)
- Article 5: “Right to Liberty”
- Article 8: “the right to respect for private and family life”, in respect of home and correspondence.

The purpose of this agreement is to provide a framework for the sharing of data, information relating to the protection of adult at risk s from abuse, in line with The Social Care Institute for Excellence’s Adult Safeguarding; Sharing Information Guide.

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 include:

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.

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 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.

Exemptions

It is not always appropriate/possible to identify a lawful basis for sharing information. Schedules 2 – 4 of The Data Protection Act 2018 set out a number of exemptions which should be considered should this be the case. This link provides an exhaustive list of these:

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

Exemptions should not routinely be relied upon or applied in a blanket fashion. You must consider each exemption on a case-by-case basis. If you cannot identify an exemption that covers what you are doing with personal data, you must comply with the GDPR as normal.

Examples:

- Prevention or detection of crime
- Court Orders
- Vital Interests (risk of serious harm or death)

European Convention of Human Rights Act 1998

These rights include Article 2: “The right to life”; Article 3: “Freedom from torture” (including humiliating and degrading treatment); and Article 8: provides that everyone has the right to respect for their private and family life, home and correspondence.

The Caldicott Principles

Principles produced by the Caldicott Committee came into being following a report on the “Review of Client Identifiable Information” in December 1997. These were then revised in 2013. Caldicott guidance applies to all NHS organisations and Local Authorities
(See Appendix 2)

The Crime and Disorder Act 1998

Section 115 provides a legal power to share information to prevent or detect crime. Some instances of abuse will constitute a criminal offence; examples of these may be assault, whether physical or psychological, sexual assault and rape, theft, fraud or other forms of financial exploitation, and certain forms of discrimination, whether on racial or gender grounds.

It is imperative that when alleged abuse is a potential criminal offence that the police are contacted as a matter of urgency. Criminal investigation by the police takes priority over all other forms of investigation.

The Mental Capacity Act 2005

A person is said to lack capacity in relation to a matter if at that point in time he/she is unable to make a decision for him/herself in relation to the matter because of an impairment or disturbance in the functioning of the brain or mind.

Capacity can fluctuate; some individuals may be able to make decisions about their daily lives but may not be able to make decisions during acute phases. Every effort should be made to assist an individual in making their own decisions by using effective communication.

The Seven Golden Rules of Information Sharing

The Seven Golden Rules for information sharing (please see Appendix 3) is an extract from HM Government 'Information sharing: Guidance for practitioners and managers', DCSF 2008.

The Golden Rules were designed to help support decision making so that information is being shared legally and professionally.

Roles and Responsibilities

All parties signed up to this agreement are committed to ensure that all staff who work with personal sensitive information understand and comply with their responsibilities to share information in accordance with the agreed Information Sharing Agreement.

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

Stockport Safeguarding Adults board 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 own organisations.

All parties have a responsibility to ensure that all members of staff are aware of this protocol and the framework for sharing personal 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.

Parties to the Agreement

As the Local Safeguarding Adult Agenda matures it may be necessary to include any other responsible body with a legal obligation and associated duty to collaborate on issues relating to Safeguarding Adults at risk.

Information to be shared

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

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

Such information may include but is not restricted to data extracted from:

- A complaint or the analysis of complaints
- An incident report or the analysis of incident reports
- The files or results of an investigation into an incident or complaint
- "Whistle-blowing" or other report of a concern relating to professional conduct or performance.
- The report or investigation of an alleged or actual criminal act relating to adults at risk.
- A report resulting from an inspection carried out by the Commission for Quality Inspectorate (CQC).

Where a concern has been raised information maybe shared that includes any of the above in addition to or contained within the following:

- Reports of a concern where evidence or information has been collated.
- The agenda, minutes and reports of an Adult Safeguarding/Protection meeting
- Letters of referral to regulatory, indemnifying or representative bodies.
- Referrals to the police.
- Minutes of meetings of the Safeguarding Adult Board.

Personal information may include:

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

How the information will be recorded and shared

Transfer of Information Verbally

- the receiver of the information is properly identified
- the receiver of the information understands their responsibility
- information is shared on a “need to know” basis only
- conversation cannot be overheard

Transfer of Information by Telephone

- the recipient is properly identified and are sure they are talking to that recipient
- the receiver of the information understands their responsibility
- information is shared on a “need to know” basis only
- conversation cannot be overheard

Transfer of Information by Fax

- use a “safe” fax machine
- phone the recipient to ensure that they are aware a confidential fax is about to be sent ,
- send a fax covering sheet to confirm correct number, confirm that the individual will wait by the machine to collect the fax and notify the sender to confirm receipt.
- keep personal information to a minimum, by using a key identifier, i.e. NHS number, social services number or unique pupil number.
- keep a log of confidential faxes sent and received

Transfer of Information by Post – Internal or External

Printed information, or other media, containing personal information will only be sent by post or via courier:

- it will be opened by the addressee only if envelope is sealed and marked “Personal & Confidential”
- When sending mail which includes sensitive personal data, use higher security mail services such as recorded or special delivery
- Full address details are used the addressee is informed the time, date and method that the information was sent and the addressee acknowledges receipt.
- Do not use internal envelopes for confidential Adult Safeguarding/Protection documents.

Transfer of Information by Email

Email is not always a secure method of sending personal sensitive information unless encryption is used. If using email:

- ensure information is kept to a minimum
- ensure it is in an attachment and that the document is encrypted and password protected
- send password details in a separate e-mail to the information
- only send on a “need to know” basis
- please note GCSX secure email is only secure to the following approved secure e-mail:

gcsx.gov.uk
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

Please note *nhs.uk **is not an** approved address

Confidentiality

The right to confidentiality is extended to all persons including clinicians, unless an organisation considers that disclosure is necessary for:

a) identifying cases in which action may need to be taken in respect of matters arising in relation to the management of an adult at risk

b) the consideration of issues relating to the taking of action in respect of
c) such matters;

d) the taking of action in respect of such matters

Retention of Records

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.

Good record keeping is an important part of the accountability of professionals. Staff that have concerns about an adult perceived to be at risk must make an Adult Safeguarding/Protection referral; this must be a full and accurate contemporaneous record of the events, their findings and concerns.

All referrals and case information will be recorded on CareFirst within the auspices of Stockport MBC/Pennine.

All hard copy referral information will be collated and archived in line with the SMBC/Pennine Record Management Policy.

Right of Access (Subject Access Requests)

The General Data Protection Regulation 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.

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

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.

All Subject Access Requests must be made in writing 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 40 days from receipt of request.

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 Stockport Metropolitan Borough Council.

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

Specialist Advice- Stockport Local Authority

In relation to Adult Safeguarding/Protection & Mental Capacity Act.	In relation to Information Sharing & Data Protection
Safeguarding Adults and Mental Capacity Act Service(Incorporating the Deprivation of Liberty Safeguards) Stockport Council-Adult Social Care **General Office Number: 0161 474-5300** **Fax: 0161 491 6118** **Email: samcas@stockport.gov.uk**	**Stockport Council Information Governance Team** **General office Number: 0161-474-4299** **Fax: 0161 474 4006** **Email: dpa.officer@stockport.gov.uk**

Appendix 1 - Key Principles of GDPR

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Appendix 2 – The Caldicott Principles (Revised 2013)

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

Principle 2 - Don't use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

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

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

In April 2013, Dame Fiona Caldicott reported on her second review of information governance, her report "Information: To Share Or Not To Share? The Information Governance Review", informally known as the Caldicott2 Review, introduced a new 7th Caldicott Principle.

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

Appendix 3 – Lawful Bases for sharing/processing personal data

The lawful bases for processing are set out in Article 6 of the 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.)

Declaration

I have read the SSAB Information Sharing protocol and agree to sign up to the requirements included within;

SIGNED _____

PRINT NAME _____

ON BEHALF OF (INSERT AGENCY) _____

DATE_____