Information Sharing Protocol
May 2017

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:

  a. The individual to whom the duty of confidentiality is owed, provides informed consents to the disclosure,

  b. There is an overriding public interest in disclosure,

  c. Disclosure is required by a court or other obligation,

  d. 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.

- **The Data Protection Act 1998**

  This Act provides the main legislative framework for confidentiality and information sharing issues. The Act stipulates eight principles (see Appendix 1) that must be followed when personal information is "processed" by organisations. The Act stipulates the conditions (i.e. the legal justifications) under which information may be shared, e.g. information may be shared if the sharing is in the legitimate interests of the person to whom the information relates.

- **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. 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 individuals 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, 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 may be 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"
- 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

Consent

Sharing with Consent

If an organisation wishes to disclose information under the agreement that contains client identifiable information but this information is not required for the purposes of identifying cases in which action may need to be taken, the organisation must remove the client identifiable information. If this is not possible or the organisation considers it necessary to disclose client identifiable information the organisation must, where practicable, obtain consent of the client to whom the information relates. In such cases only the minimum amount of person identifiable information will be disclosed.

Other Justifications for Sharing

It is not always appropriate/possible to obtain consent as the basis for sharing information, the following justifications under Safeguarding Adults may become applicable:

Serious harm

It may be justified to share information where there is evidence that serious harm would be caused to the service user, (or another person) if this was not done.

Vital interests

Information may be shared where this is in the “vital interests” of the adult at risk or another person. This refers to life or death circumstances.

Prevention or detection of crime

Personal information may be provided to the Police where this is necessary for the prevention or detection of crime. This is a **power not an obligation**. A judgement needs to be made in each case as to whether it is appropriate to release information taking into account the following criteria. Advice should be sought, if there is uncertainty about interpreting these criteria.

Information should only be disclosed where:

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

Court Order

Information must be shared where the service is instructed to do so by a Court (including a Coroner’s Court.)Wherever possible and appropriate adults at risk should be informed if their information is to be shared without consent.

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 such matters;

(c) the taking of action in respect of such matters

Retention of Records

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.

Subject Access Requests

The Data Protection Act 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

The Partner Organisations will review this protocol 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 Data Protection Act 1998 can be accessed via the Information Commissioner's website at www.informationcommissioner.gov.uk
- 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 Data Protection Act 1998

1. Fair and lawful: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met, also the processing must adhere to the fair processing code.

2. Use for specified purposes: Personal data shall be obtained only for one or more specified purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.

3. Adequate, relevant and not excessive: Personal data shall be adequate, relevant and not excessive in relation to the purpose.

4. Accurate and up to date: Personal data shall be accurate and, where necessary, kept up to date.

5. Don't keep longer than necessary: Personal data processed for any purpose or purposes shall not be kept longer than is necessary for the purpose of those purposes.

6. Rights given under the act: Personal data shall be processed in accordance with the rights of the data subject under this act.

7. Security: Appropriate and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Disclosure outside Europe: Personal data shall not be transferred to a country outside the European Economic area, without adequate protection

Appendix 2 – The Caldicott Principles

Principle 1: Justify the purpose(s)

Every proposed use or transfer of personally identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appropriate guardian.

Principle 2: Do not use personally identifiable information unless it is absolutely necessary.

Personally, identifiable information items should not be used unless there is no alternative.

Principle 3: Use the minimum personally identifiable information.

Where the use of personally identifiable information is considered essential, each individual item of information should be justified with the aim of reducing identifiably.

Principle 4: Access to personally identifiable information should be on a strict need to know basis.

Only those individuals who need access to personally identifiable information should have access to it.

Principle 5: Everyone should be aware of their responsibilities.

Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and obligations to respect patient/client confidentiality.

Principle 6: Understand and comply with the law.

Every use of personally identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

Appendix 3 – The Seven Golden Rules for Information Sharing

1. **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.

2. **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be, shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.

4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

5. **Consider safety and wellbeing:** base your information-sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions.

6. **Necessary, proportionate, relevant, accurate, timely and secure:** ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely.

7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

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_____