Information sharing guide and protocol

Version 1 • August 2020

Document properties	Version details
Document name	Information sharing guide and protocol
Document owners	Brighton & Hove, East Sussex and West Sussex Safeguarding Adults Boards
Version	1 – Final
Previous version	N/A
Review plan	The protocol will be reviewed by representative(s) nominated by the Brighton & Hove, East Sussex and West Sussex SABs on an annual basis.
Review date	August 2021

Contents

The seven golden rules to sharing information

1.	GDPR and the Data Protection Act 2018 and human rights legislation are **not barriers** to justified information sharing but provide a framework to ensure that personal information about individuals is shared appropriately.
2.	Be **open and honest** with the adult (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** from other practitioners, safeguarding leads or information governance leads if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4.	Share information with **informed consent,** where appropriate, and where possible, but respect the wishes of those who do not consent to share confidential information. **There is a lawful basis to share information without consent** if, in your judgement, there is good reason to do so, such as where **safety may be at risk**. Base your judgement on facts.
5.	Consider safety and well-being. **Base your information sharing decisions on considerations of the safety and well-being** of the adult and others who may be affected by their actions.
6.	**Necessary, proportionate, relevant, adequate, accurate, timely and secure:** Ensure the information you share is necessary for the purpose for which you are sharing it, shared only with those individuals who need to have it, is accurate and up-to-date, shared in a timely fashion, and shared separately.
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.

The seven Caldicott principles

Justify the purpose(s). Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented.

Don’t use personal confidential data unless it is absolutely necessary.

Use the minimum necessary personal confidential data.

Access to personal confidential data should be on a strict need-to-know basis.

Everyone with access to personal confidential data should be aware of their responsibilities.

Every use of personal confidential data must comply with legal requirements.

The duty to share information can be as important as the duty to protect confidentiality.

Introduction

The Safeguarding Adults Boards (SABs) across Brighton & Hove, East Sussex and West Sussex are committed to the effective sharing of information to safeguard and promote the welfare of adults at risk of abuse and neglect, and to improving outcomes for all.

This Information Sharing Guide and Protocol covers the sharing of information between partner agencies of the Sussex SABs for the purposes of safeguarding adults. This agreement is a means of establishing a standard for sharing sensitive and confidential information and for ensuring those making decisions about adults who may be at risk of abuse or neglect is conducted within statute and regulatory guidance. This protocol in itself does not give partners an automatic right to receive information or a mandate to provide information; it instead formalises the process in which information is shared in situations when it is suitable to be shared.

The sharing of information must only happen when it is legal and necessary to do so, and adequate safeguards are in place to protect the security of the information. This guide and protocol have been updated to comply with relevant legislation and reflect the General Data Protection Regulation (GDPR) and Data Protection Act 2018. Good practice guidance has also been consulted as follows:

- The Information Commissioner's Data Sharing Code of Practice.
- HM Government Information Sharing: Advice for practitioners providing safeguarding services.

This guide and protocol should be read together with any individual agency procedure governing information sharing to safeguard adults with care and support needs. Individual information sharing agreements for specific purposes are developed where required on a case-by-case basis.

Purpose of this guide and protocol

This guide and protocol provides a framework for the secure and confidential sharing of information between organisations to:

- Ensure there is a consistent and effective response to safeguarding concerns and allegations or disclosures of abuse or neglect.
- Work efficiently together to conduct safeguarding enquiries and support other reviews, such as Safeguarding Adults Reviews.

Information sharing supports three important aspects of multi-agency safeguarding working:

- **Understanding the problem** – understanding the issues associated with abuse and neglect requires information to be brought together from a range of agencies. This involves exploring patterns relating to the problem, and then deciding on tactical, investigative or strategic responses to support those adults at risk of harm from abuse or neglect.

- **Multi-agency in content, multi-agency in outlook** – considering the issue using information from a range of agencies rather than just one agency leads more naturally to a multi-agency response and joined-up approach to addressing the issue.

- **Supporting partnership working** – information sharing helps to foster and improve inter-agency relationships and leads to a more co-ordinated response.

Parties to this protocol

The parties to this protocol are those listed in Appendix 1 and have signed the Declaration of Acceptance and Participation (see Appendix 2). The declaration will be signed by service directors or the equivalent functional heads of each organisation.

Legal basis for information sharing

If you are asked to or wish to share information about an adult who may be experiencing or is at risk of abuse or neglect, you need to have a good reason or legitimate purpose to share information.

All organisations are subject to a variety of legal, statutory and other guidance in relation to the sharing of person-identifiable or anonymised data. Whether you work for a statutory service or within the private or voluntary sector, any sharing of information must comply with the law relating to confidentiality, data protection and human rights. Establishing a legitimate purpose for sharing information is an important part of meeting those requirements.

The key legislation which underpins the sharing of information includes (this is not an exhaustive list):

- General Data Protection Regulation (GDPR) and Data Protection Act 2018

- The common law duty of confidentiality
- Human Rights Act 1998
- Crime and Disorder Act 1998
- Mental Capacity Act 2005
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Criminal Justice Act 2003
- Care Act 2014

Each of these pieces of legislation and any other legislation of relevance must be considered when deciding whether information can be shared.

In general, the law will not prevent the sharing of information with other agencies and practitioners if:

- those likely to be affected give consent; or
- the public interest in safeguarding the welfare of the adult at risk of harm overrides the need to keep the information confidential; or
- disclosure is required under a court order or other legal obligation; or
- sharing information is required for detection or prevention of crime.

GDPR and Data Protection Act 2018

The GDPR and Data Protection Act 2018 introduce new elements to the data protection regime, superseding the Data Protection Act 1998. Practitioners must have due regard to the relevant data protection principles which allow them to share personal information appropriately.

The GDPR and Data Protection Act 2018 place greater significance on organisations being transparent and accountable in relation to their use of data. All organisations handling personal data need to have comprehensive and proportionate arrangements for collecting, storing, and sharing information.

To effectively share information:

- All practitioners should be confident of the processing conditions, which allow them to store, and share, the information that they need to carry out their safeguarding role. Information which is relevant to safeguarding will often be data which is considered 'special category personal data' meaning it is sensitive and personal.

- Where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent.

- Information can be shared legally without consent, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place the individual at risk.

- Relevant personal information can be shared lawfully if it is to keep an adult at risk safe from abuse or neglect, or if it is protecting their physical, mental or emotional well-being.

Each signatory organisation must respect the rights of individuals with respect to their personal data and must adhere to the principles of the GDPR and Data Protection Act 2018 both in terms of processing personal information with another signatory agency for the purpose of this protocol and with organisations or individuals who are not signatories to this agreement.

The GDPR principles specify that personal data must be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

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;

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

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

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 is 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; and

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.

Where possible, the data protection principles must be adhered to, but it may be worth considering the social care exemptions in Schedule 3 of the Data Protection Act 2018, which exclude the data protection principles "to the extent necessary" to avoid causing serious harm.

Additional information is available on the Information Commissioner's Office website.

Common law duty of confidentiality

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

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

The sharing of information across partner agencies of the Sussex SABs is guided by the Caldicott principles as outlined at the beginning of this guide.

Freedom of Information Act 2000

Under the Freedom of Information Act, the public can write to any public authority designated under the Act to request any recorded information that is held by that authority.

Since SABs are not public authorities as defined by the Act, any Freedom of Information request submitted to the Brighton & Hove, East Sussex or West Sussex SABs will need to be dealt with under the umbrella of the relevant Council Freedom of Information process.

Further information about Freedom on Information requests can be found on the following website pages:

- Brighton and Hove City Council
- East Sussex County Council
- West Sussex County Council

Criminal Justice Act 2003

The Criminal Justice Act 2003 provides for the establishment of Multi-Agency Public Protection Arrangements (MAPPA) in each of the 42 criminal justice areas in England and Wales. These are designed to protect the public, including previous victims of crime, from serious harm by sexual and violent offenders. They require the criminal justice agencies and other agencies to work in partnership in dealing with offenders, including sharing of information which must be in accordance with the law.

Police, Prison Service, and Probation Trusts are 'Responsible Authorities'.

The Brighton & Hove, East Sussex and West Sussex Local Authorities, Sussex Partnership NHS Foundation Trust, East Sussex Healthcare NHS Trust and the Sussex Clinical Commissioning Groups are 'Duty to Cooperate Agencies' under MAPPA procedures and there is a statutory basis for information sharing. These agencies are members of the SAB. The SAB includes other agencies who are not 'Duty to Cooperate Agencies' under MAPPA procedures, but who may be required by MAPPA to share information. Section 325(4) of the Criminal Justice Act 2003 expressly permits the sharing of information between agencies for MAPPA purpose of public protection.

Common Law Police Disclosures (CLPD)

The CLPD provisions allow forces to proactively provide personal data or sensitive personal data to a third party, using common law powers. The provisions relate to the circumstances in which the police can disclose information they hold regarding an individual in order to enable a third party to consider risk mitigation measures in respect of an employment or voluntary role believed to be undertaken by that individual.

The scheme provides robust safeguarding arrangements whilst ensuring that only relevant information is passed onto employers. This scheme strikes an appropriate balance between the interests of the individual and the importance of public protection.

Any consideration or request for CLPD should ensure that this is compliant with other legislation, including GDPR, and that a pressing need to share information can be justified and recorded.

Further information can be accessed via the College of Policing website.

Care Act 2014

Sharing information between organisations as part of day-to-day safeguarding practice is not expressly covered in the Care Act because it is already addressed by the common law duty of confidentiality, the Data Protection Act 2018 and the General Data Protection Regulation 2018, the Human Rights Act 1998 and the Crime and Disorder Act 1998.

Under the Care Act a local authority must:

- Set up a SAB to share strategic information to improve local safeguarding practice.
- Cooperate with each of its relevant partners; each relevant partner must also cooperate with the local authority.

Section 45 of the Care Act 2014 introduced a specific provision regarding the supply of information to SABs if conditions are met. A SAB may request a person to supply information to it or another person, and the person who receives the request must provide the information 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 or
  - the information requested has already been passed onto another person subject to this requirement.

This reflects that information sharing is essential to improve outcomes for all and to ensure issues for wider public protection as well as risk to individuals are detected.

In line with a Making Safeguarding Personal approach, the Care Act emphasises the need to empower people, to balance choice and control for individuals against preventing harm and reducing risk, and to respond proportionately to safeguarding concerns. The Mental Capacity Act 2005 is also relevant as those coming into contact with adults with care and support needs should be able to assess whether someone has the mental capacity to make a decision concerning risk, safety or sharing information.

Types of information shared

The signatories to this protocol may need to share the following types of information:

Personal information

This is information, as defined by the Data Protection Act 2018 and the General Data Protection Regulations 2018, relating to a living individual who can be identified either from that information or from that information in conjunction with other information that is in, or is likely to come into, the possession of the data holder. Personal information is technology neutral eg. on a computer database, paper filing system, microfiche, portable memory stick.

Depersonalised information

Depersonalised information includes any information that does not and cannot be used to establish the identity of a living person, having had all identifiers removed and is outside the remit of the Data Protection Act 2018 and the General Data Protection Regulations 2018.

Aggregated (statistical) information

Non-personal information does not refer to individuals and is outside the remit of the Data Protection Act 2018 and the General Data Protection Regulations 2018. However, some aggregated information may be of a sensitive nature.

Issues of confidentiality and consent

Confidential personal information may be shared if consent to share has been given by the confider or data subject. This should be sought if it is safe or appropriate and feasible to do so. An informed consent-based approach is always a preferred option.

In situations when the individual, about whom the data relates to, does not have capacity to give consent to the sharing of information, then a best interests decision should be made in line with the principles of the Mental Capacity Act.

The Caldicott Committee Report on the review of patient-identifiable information recognises that confidential information may sometimes need to be disclosed in the best interests of an individual and outlines principles to safeguard this information sharing as follows:

- information will only be shared on a 'need to know' basis when it is in the best interests of the adult,
- confidentiality must not be confused with secrecy,
- informed consent should be obtained but, if this is not possible and other adults are at risk of abuse or neglect, it may be necessary to override the requirement; and,
- it is inappropriate for agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other vulnerable people may be at risk.

Decisions should be proactively taken based on professional judgement and proportionality. It is recognised that both organisations and individuals have a professional responsibility to share information and that this duty will outweigh the duty of confidentiality owed to the individual.

Any decisions to share information taken in these circumstances must be fully documented with clear justification and decision making and involving Caldicott Guardians where necessary.

If it is not possible to obtain consent before sharing information, the data subject or confider should be informed as soon as possible after the information has been shared, unless it would be inappropriate to do so. There are some circumstances in which it is not appropriate to seek consent to share information and / or inform the adult that information is being shared, for example if doing so:

- would place the adult concerned at risk of significant harm,
- would prejudice the prevention, detection or prosecution of a crime, or
- would lead to an unjustified delay in carrying out an enquiry into the abuse or neglect.

Client consent is not necessary for sharing depersonalised / anonymous data from which individuals cannot be identified or for sharing aggregated data.

Information security, retention and disposal of information

Confidential and personal information will be held in line with the GDPR and Data Protection Act 2018. Each signatory organisation will need to have the appropriate level of security in place which is in line with the sensitivity and classification of the information to be shared and stored. Information shared for the purpose of safeguarding adults should not be used by partner agencies for any other purpose without the consent of the originator.

Personally identifiable information will only be shared using secure e-mail, such as Voltage Secure Mail with password protected documents.

Each signatory to this protocol will need to ensure that appropriate technical and organisational measures are in place to protect against unauthorised or unlawful processing of personal information and against accidental loss or destruction, or damage to personal information.

Information will be securely stored by each agency and each agency will undertake to securely delete any information once it is no longer required. Each signatory organisation must ensure that system-specific policies and mechanisms are in place to address access levels, physical security of information, security awareness and training and security management, systems development and data transfer and transport.

Information governance

Each signatory organisation will have appropriate information governance in place and / or operational policies and procedures that will facilitate effective and secure processing of information.

Non-compliance and breaches of security

Instances of internal non-compliance and breaches relating to information shared as a result of this protocol must be logged and reported to the relevant SAB. Any non-compliance or breach must be dealt with promptly in accordance with the organisation's information governance or operational procedures, and notified to the relevant owning agency within 24 hours.

Incidents relating to information shared as a result of this protocol that should be logged and reported include, but are not restricted to:

- refusal to disclose information to signatories
- conditions being placed on disclosure
- disregard of agreed policies and procedures
- disregard of the views and rights of service users
- inappropriate, unauthorised or unlawful disclosure
- inappropriate or unauthorised access
- theft, loss or damage to information or other breaches of security.

Sharing safeguarding information between partner agencies

The Care Act recognises that safeguarding individuals requires multi-agency responsibility and emphasises the need for co-operation and partnership work. The local authority has the lead responsibility for safeguarding adults with care and support needs, and the police and NHS also have clear safeguarding duties under the Care Act. Partner agencies often have different geographical boundaries or IT systems, for example, which can create complexities with regards to information sharing in practice.

Safeguarding Adults Reviews frequently highlight failures between safeguarding partners in terms of effective communication, recording and sharing information and collaborative working. Some practitioners can be over-cautious about sharing

personal information, particularly if it is against the wishes of the individual concerned. They may also be mistaken about needing evidence or consent to share information. The risk of sharing information is often perceived to be higher than it actually is. It is important that practitioners consider the risks of not sharing information when making decisions.

The statutory guidance to the Care Act emphasises the need to share information about safeguarding concerns at an early stage, and this is key in providing an effective response where there are emerging concerns about abuse or neglect. When safeguarding concerns are raised with the local authority, wherever appropriate, referring agencies should be given feedback as to the outcome of how safeguarding concerns are being progressed.

Safeguarding meetings / discussions

Whilst the flexible approach to safeguarding under the Care Act means that a formal meeting may not always be required, meetings are often the best way to ensure effective co-ordination across all agencies. All meetings held under the Sussex Safeguarding Adults Policy and Procedures must adhere to boundaries of confidentiality. The following good practice principles support effective multi-agency information sharing in the context of safeguarding meetings:

Ensure that **all** relevant agencies are involved in safeguarding meetings and discussions. Always consider sharing information and sending invitations to safeguarding meetings with primary care agencies, such as the GP.

Invitations and documentation required for safeguarding meetings should be sent securely, with appropriate Government Security Classification, and with sufficient notice ahead of the meeting. Details of those who have been invited should be clearly recorded.

All agencies invited to safeguarding meetings have a responsibility to attend. Where the individual cannot attend, they should inform the meeting organiser and arrange for an alternative representative from their agency to attend if possible. Notes of meetings should document all those in attendance, as well as those who are unable to attend.

Minutes of meetings / discussions should be shared with all agencies invited regardless of whether the agency representative has been able to attend the meeting. In situations when apologies for meeting attendance have not been received it is good practice to ensure meeting minutes are still circulated to that agency representative.

All agencies have a responsibility to share any information they have which may be relevant to safeguarding the adult. Where representatives from key agencies are absent from meetings, where possible they should provide information in advance. The lead professional / Chair should ensure that agencies absent from meetings are kept informed of outcomes, and any agreed actions and timescales allocated to them.

Record keeping and data quality

Good record keeping is a vital component of effective safeguarding practice and minutes should be factual, objective, clear and accurate.

Minutes form part of the adult's information and as such are governed by data protection legislation. Safeguarding minutes are intended to be confidential and should not be released without the consent of all parties. All documentation should be marked as 'confidential'.

Once minutes have been agreed by the chair of the meeting, they should be circulated to all agency representatives in draft, providing the opportunity for comment before they are finalised. A date by which comments should be sent back should be clearly stated.

The contents of the safeguarding meeting minutes should not be discussed with any third party without the consent of the chair.

Each signatory organisation is responsible for the quality of the personal data it obtains, records, holds, uses and shares and will have appropriate procedures in place for monitoring and ensuring standards. All signatories receiving shared information are responsible for applying relevant data quality checks before using the information. Partners to this protocol will notify the source of the information if they discover that the information is inaccurate or inadequate for the purpose. The source will be responsible for correcting the data and notifying all other recipients in writing.

Sharing of information within Single Combined Assessment of Risk Form (SCARF)

Sussex Police has a direct referral process for police officers to raise a safeguarding concern with the local authority. The Vulnerable Adult at Risk (VAAR) section of the Single Combined Assessment of Risk Form (SCARF) should be completed by the police for every safeguarding concern. It is important that when the police are completing a SCARF that they add sufficient and accurate detail to allow specialist teams and the local authority to act on it. The expectation is that the submitting officer will also state on the form why they are making the referral and whether the adult at risk is aware of this.

SCARFs may only be shared by other agencies in their entirety with partners of the Sussex SABs (as outlined in Appendix 1). SCARFs may only be shared with a third-party organisation who is not a member of the relevant SAB with the written consent of Sussex Police.

Review of this guide and protocol

The protocol will be reviewed by representative(s) nominated by the Brighton & Hove, East Sussex and West Sussex SABs on an annual basis and will also be reviewed in the event of any relevant change in law, or changes in the circumstances relevant to the agreement.

Appendix 1: Partners of the Sussex Safeguarding Adults Boards

Partners of the Brighton & Hove Safeguarding Adults Board

- Brighton & Hove Health and Adult Social Care
- Sussex Clinical Commissioning Groups
- Sussex Police
- Age UK Brighton & Hove
- Brighton and Hove City Council (BHCC) Children's Social Care
- BHCC Community Safety
- BHCC Health, SEN and Disabilities
- BHCC Housing
- BHCC Lead Member for Adult Social Care
- BHCC Public Health
- Brighton and Sussex University Hospital NHS Trust
- Brighton Housing Trust
- Brighton Oasis Project
- Care Quality Commission
- Cranstoun
- East Sussex Fire and Rescue Service
- Healthwatch
- Kent, Surrey, Sussex Community Rehabilitation Company
- Money Advice Plus
- National Probation Service
- NHS England
- South East Coast Ambulance Service NHS Foundation Trust
- Sussex Community NHS Foundation Trust
- Sussex Partnership NHS Foundation Trust

Partners of the East Sussex Safeguarding Adults Board

- East Sussex Adult Social Care and Health
- Sussex Clinical Commissioning Groups
- Sussex Police
- Care for the Carers
- Care Quality Commission
- Change, Grow, Live (CGL)
- District and Borough Councils
- East Sussex County Council (ESCC) Children's Social Care
- ESCC Trading Standards
- East Sussex Safeguarding Children Partnership
- East Sussex Fire and Rescue Service
- East Sussex Healthcare NHS Trust
- Healthwatch
- Her Majesty's Prison Service (HMPS) Lewes
- Kent, Surrey, Sussex Community Rehabilitation Company
- Lay members
- National Probation Service
- NHS England
- Registered Care Association
- South East Coast Ambulance Service NHS Foundation Trust
- Sussex Community NHS Foundation Trust
- Sussex Partnership NHS Foundation Trust
- Voluntary and community sector representation

Partners of the West Sussex Safeguarding Adults Board

- West Sussex County Council
- Sussex Clinical Commissioning Groups
- Sussex Police
- Brighton and Sussex University Hospital NHS Trust
- Care Quality Commission
- District and Borough Councils
- HMPS Ford
- Local Safeguarding Children's Board
- National Probation Service
- NHS England
- Queen Victoria Hospital
- South East Coast Ambulance Service NHS Foundation Trust
- Surrey and Sussex Healthcare
- Sussex Community Foundation NHS Trust
- Sussex Partnership NHS Foundation Trust
- West Sussex County Council (WSCC) Community Safety and Wellbeing
- WSCC Lifelong Services
- WSCC Public Health
- West Sussex Fire and Rescue Service
- Western Sussex Hospitals NHS Foundation Trust
- West Sussex Partners in Care
- Voluntary and community sector representation

Appendix 2: Declaration of acceptance and participation

Information sharing guide and protocol

Declaration of acceptance and participation

Effective from 10th August 2020

Signed by, for and on behalf of:

Organisation	
Name	
Position	
Contact details including address, email and telephone number	
Signature	
Date	
Organisational contact for information sharing	
Position	
Contact details including address, email and telephone number	