Protocol for Information Sharing in Southwark

For agencies working with children, young people, parents and carers in Southwark

Southwark Safeguarding Children Board
September 2015

Contents

1. Introduction

1.1 This protocol is based on '*Working Together 2015'* and '*Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers 2015' and* sets out the principles for the legal, secure and confidential sharing of personal information among partner organisations in the London borough of Southwark.

Sharing information is an intrinsic part of any front line practitioner's job when working with children and young people and decisions about how much information to share, with whom and when, can have a profound impact on individual's lives.

It can be the key to providing effective early help to families where there are emerging problems or at the other end of the continuum, sharing information can be essential to the protection of children. Poor or non-existent information sharing is a factor that has repeatedly been flagged up in Serious Case Reviews following the death or serious injury of a child.

1.2 Information sharing is a positive act when it is done for the good of children, young people and their families, but practitioners and managers need to be aware of thresholds and permissions, especially if without the owner's consent.

1.3 The Data Protection Act 1998 encourages local areas to establish information sharing governance frameworks to set out the principles and legislation we are obliged to adhere to when handling personal information.
This protocol sets out the commitment of all partners who have signed it to sharing information in order to improve outcomes for children, young people and their families. It outlines the principles and standards of expected conduct and practice of partner organisations and staff who work for them, and aims to dispel any misunderstandings, for example the role of the Data Protection Act.

1.4 This protocol applies to all personal information handled by partner organisations including but not limited to information held on manual records and information processed electronically by computer, CCTV or audio recordings.

1.5 For the purposes of this protocol, there are two 'types' of information sharing, which are dealt with in different ways:

Bulk or pre-planned sharing

The information commissioner's office says: "An information sharing protocol is a useful tool with which to manage large-scale, regular information sharing. It creates a routine for what will be shared, when and with whom, and provides a framework in which this regular sharing can take place with little or no intervention by practitioners.

"It is not a useful tool for managing ad hoc information sharing which all practitioners find necessary. Most importantly it is not intended to be a substitute for the professional judgement which an experienced practitioner will use in those cases and should not be used to replace that judgement."

This type of information sharing is governed by the guidance in Section 2.

Case-by-case decisions

Practitioners must use their professional judgement and experience to make decisions on a case-by-case basis, as to whether and what personal information they should share with other practitioners in order to meet the needs of a family. The decision to share information lies in the practitioner's professional judgement, guided by the principles in this framework and the legal framework outlined in Section 4.

This type of information sharing is governed by the guidance in Sections 6 and 7.

1.6 Who is covered by this framework?

A list of the organisations that have signed up to this framework is set out on page 23. Agencies that are commissioned or funded by statutory partners would be expected to follow its principles. Even if your organisation has not signed up to it, this framework provides guidance which you may find helpful and will help you understand the standards partner organisations apply. This framework also provides guidance to clients and 'data subjects' so that they know what their rights are and what standards they can expect from partner organisations.

1.7 How does this framework work with my own organisation's procedures?

All agencies that are party to this protocol agree to take individual responsibility for monitoring and reviewing the implementation of the protocol in their organisations.

2. Seven golden rules for sharing information

The seven golden rules for information sharing, as set out in the national guidance:

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 person 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 persons 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.

3. Information sharing principles

Partner organisations of Southwark Safeguarding Children Board agree to ensure compliance with the following key principles:

1. To share information in a timely manner where it is lawful to do so
Partner organisations recognise that sharing personal information is essential for child protection and promoting the welfare of children and young people, enabling early intervention and preventative work and for wider public protection. Each partner will be pro-active in making available information that might assist the specific or shared priorities of partners. Each partner will nominate a senior representative to champion information sharing internally and to work with partners on the implementation and development of the protocol. All partners demonstrate their acceptance to the minimum standards set out in this code by signing the declaration on page xxx.

2. To comply with statutory duties
Partner organisations are fully committed to ensuring that they share information in accordance with their statutory duties, including the requirements of the Data Protection Act 1998 and the Human Rights Act 1998.

3. Professional judgement
Partner organisations recognise that decisions to share information on a case-by-case basis which are not clearly covered by statute must always be based on professional judgement about the consent and/or safety and wellbeing of the person. Agencies will provide staff with the guidance, training and support to enable them to make these decisions.

4. Caldicott requirements
Partner organisations recognise the requirements that Caldicott imposes on NHS organisations and social care provision. They will ensure that requests for information from these organisations are dealt with in a manner compatible with these requirements.

5. Duty of confidentiality
All organisations party to this framework recognise the importance of the legal duty of confidentiality, and will not disclose information to which this duty applies without the consent of the person concerned, unless there are statutory grounds or an overriding

public interest justification for so doing. In requesting release and disclosure of information from partner organisations, all staff will respect this responsibility.

6. Consent

Partner organisations will seek consent from the service user to share personal information unless to do so would create or increase risk of harm. Where consent to disclose information is requested, the service user will be made fully aware of the information it is proposed to share and the purposes for which it will be used. If a person is unwilling to give consent, information will be shared only where there are appropriate statutory or public interest grounds for doing so.

7. The voice of children and young people

Partner organisations will ensure that staff explain the issues relating to the sharing of personal information to children and young people in a way that is suitable for their age, language and likely understanding. Where a child or young person is judged not to have the capacity to understand and make their own decisions, and hence to consent to the sharing of personal information, their views will still be sought as far as possible.

8. Sharing without consent

Partner organisations will ensure that decisions to share personal information without consent are fully considered and comply with the requirements of the relevant legislation. All relevant staff will be provided with training to enable them to share information appropriately, legally and professionally.

9. Necessary and proportionate

When taking decision about what information to share, partner organisations will consider how much information needs to be released. The date protection act requires agencies to consider the impact of disclosing information on the information subject and any third parties. Any information sharing must be proportionate to the need and level of risk.

10. Specific purpose

Partners will not abuse information that is disclosed to them. Information shared with a member of another organisation for a specific purpose will not be regarded by that organisation as intelligence for the general use of the organisation. All partner organisations are also aware that information shared may be used in legal proceedings in order to safeguard the welfare of the child.

11. Accuracy

Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

12. Access to information

People will be fully informed about the information that is recorded about them. They will be able to gain access to information held about them and to correct any factual errors that may have been made. If an organisation has statutory grounds for restricting a person's access to information about them, they will be told that such information is held and the grounds on which it is restricted.

14. Security

Partner organisations will implement measures to ensure the secure storage, access and transfer of all personal information retained within their manual and/or electronic systems. Wherever possible, information should be shared in an appropriate, secure way. Practitioners must always follow their organisation's policy on security for handling personal information.

15. Complaints procedures

Partner organisations are committed to having procedures in place to address complaints relating to the disclosure of information. Service users will be provided with information about these procedures.

16. Staff awareness

Partner organisations will ensure that all relevant staff are aware of and comply with their responsibilities in relation to:

This protocol

The confidentiality of information about service users

The commitment to share information in accordance with guidance and legislation

17. Implementation, monitoring and review

Partners will participate in the implementation, monitoring and improvement of the use of this protocol and will ensure that it is widely circulated in their organisation and will provide appropriate staff training as required.

4. The legal framework

4.1 In general individuals have a right to choose how their personal data is used and who may have access to it. However the law allows for information to be shared where there is a legitimate purpose and a legal basis for doing so.

4.2 Public bodies require administrative powers to share information for specific purposes and these powers will often be provided by a statutory provision which sets out the legal basis for disclosure.

4.3 The principle laws concerning the protection, disclosure and use of personal information include:

The data protection Act

The Human Rights Act

The Freedom of Information Act

The common law duty of Confidence

The Caldicott principles

The Children Act 2004

See Appendix 1 for more detailed information about these.

5. Information sharing guidance

5.1 Types of personal information

For the purposes of this framework these terms are defined as follows:

Personal information means data which relate to a living individual who can be identified:

- From the data
- From the data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

Sensitive information means personal data consisting of information as to:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Whether they are a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992)
- Their physical or mental health or condition
- Their sexual life
- The commission or alleged commission by them of any offence Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings

Depersonalised data means any information that does not and cannot be used to establish the identity of a living individual and has had all personal identifiers removed.

For children and young people under the age of 16, a person with parental responsibility can give consent for that child.

When information sharing is required in relation to a **deceased person**, the Data Protection Act does not apply. In these circumstances the general principles of this framework and the Access to Health Records Act will be applied. Careful consideration will be given to the disclosure of information concerning a deceased person and, if necessary, legal advice should be sought on each individual case.

Notification

Each agency must ensure their notification with the information commissioner permits the collection, use and sharing of data under its specific purpose.

5.2 Security of information

All partners will take any necessary steps to ensure the personal data held by them, both paper and electronic records, are held securely and are available only to other agencies on a 'need to know' basis. This will include the use of data memory sticks and/or laptops as well as fixed computers.

Each partner agrees to transmit information securely and by so doing certifies that those methods are compliant with the Data Protection Act. This will include secure or encrypted emails or password-protected documents.

Each recipient must ensure the information is securely stored and when it has served its purpose it must be destroyed as confidential waste, under the agency's retention of records policy.

5.3 Information management and security breaches

Guidance regarding data security is available on the Southwark Safeguarding Children Board web pages.

Notification of data security breaches to the Information Commissioner's Office

Although there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the information commissioner believes serious breaches should be brought to the attention of his office. Although 'serious breaches' are not defined, the following should assist in a decision about whether breaches should be reported:

• **Potential harm to data subjects** Where there is a significant actual or potential harm as a result of the breach, whether because of the volume of data, its sensitivity or a combination of the two, there should be a presumption to report.

• **Volume of personal data lost, released or corrupted** There should be a presumption to report where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. A large volume would generally be any collection containing information about 100 or more individuals.

• **Sensitivity of data lost, released or unlawfully corrupted** There should be a presumption to report where smaller amounts of personal data is involved which could cause a significant risk of individuals suffering substantial harm. This is most likely to be the case where that data is sensitive personal data as defined in Section 2 of the Data Protection Act.

5.4 Supply and accuracy of information

Children, young people and their parents/carers have the opportunity to gain access to information held about them, in accordance with the Data Protection principles, and to correct any factual errors that have been made.
Where an agency finds that the information it has disclosed is inaccurate, that partner shall advise the corrections that need to be made to all other partners that it knows has received or holds that information. Each partner must ensure that the correction is made to its records.

5.5 Use of statistical and anonymous data

Section 33 of the Data Protection Act provides for various exemptions in respect of the processing or further processing of personal data for “research purposes”. This includes processing for statistical or historical purposes, provided the data are not processed to support measures or decisions relating to particular individuals and are not processed in such a way that substantial damage or distress is caused or likely to be caused to any data subject.

Where processing for research, historical or statistical purposes, data controllers should always consider whether it is necessary to process personal data in order to achieve their purpose. Wherever possible, data controllers should only process data that has been stripped of all features which could lead to the identification of a data subject. Partner organisations will request permission from the originating data controller, if they wish to use information for any purpose other than that for which the information was originally provided, including providing other organisations with statistical data derived from service user records.

Partner agencies publishing reports, including aggregated data drawn from case records or case studies, should ensure that such report are DPA compliant and anonymised. Partner organisations must not attempt to identify a living individual from the collation of anonymised data. Consideration must be given prior to release as to whether it would be possible to identify an individual from that data, should it be disclosed, or if further information were added to it.

It is important that data subjects are informed from the outset, as to the purposes for which their data may be processed, in order to avoid the data subject being misled as to the purposes for which consent was given.

5.6 Retention of information

Partners will ensure that all data obtained from any other partner are retained only for as long as they are required to achieve the purposes for which they were initially provided. It will be the responsibility of the recipient agency to ensure that all data are relevant, accurate and up to date. Agencies should have clear retention policies which include the frequency for review of whether data should be retained.

5.7 Recording reasons for disclosure of information

Staff working with children and parents need to take professional decisions based on their understanding of the law and the particular situation, and record their decisions and reasons for sharing information.
Good information sharing is based on good record keeping. Records should be accurate, relevant, up to date and kept for no longer than is necessary for their purpose.
Each partner will have their own file retention and recording procedures and will ensure that these will be compliant with the relevant legislation and guidance. It is important that these procedures are shared with partner agencies and service users.

5.8 Secondary disclosure

Each partner will always retain ownership of the personal information it discloses to another partner. The identity of the originator must be recorded against the relevant information. A recipient of the information must obtain the consent of the original information owner before making a further disclosure to a secondary person or body, ie an agency outside this framework.

Permission must also be obtained before using the information for a different purpose from that which it was first obtained, even if permission has been received from the data subject. Information must not be disclosed to any non-agency body or person without first obtaining the consent of the data owner and seeking legal advice.

5.9 Safe and confidential transfer of information

Each partner agency agrees to facilitate the exchange of information in a secure manner, by adopting a classification policy that defines acceptable processes when exchanging Information via post, email, fax, telephone and couriers etc.

Any agencies or organisations not able to use encrypted electronic systems will ensure that any information to be shared electronically is sent via a password protected e-mail system. When faxing information, only safe haven faxes should be used. When transferring information by telephone, the identity of the caller and their right to the Information should be checked and

confirmed. In meetings where confidential information is shared, the minutes of the meeting should note that the information is not to be shared.

6. Privacy, confidentiality and consent

6.1 Consent

Consent should always be sought where appropriate. This means that users must be informed why information may need to be shared and why particular actions need to be taken, unless to do so would adversely affect the purpose for which the information is to be shared. Many of the data protection issues surrounding disclosure can be avoided if the consent of the individual or the parent/carer has been sought and obtained. It shall be normal working practice in each partner agency to obtain the consent of the child or young person where able to give informed consent and/or their parent prior to disclosing information about them to another agency. The exception to this is where this would put someone at risk of harm or prejudice a police investigation into a serious offence, or lead to unjustifiable delay in protecting a child.

For consent to be valid, it must be:
• **Fully informed -** the individual is aware of what information will be shared, with whom and for what purpose.
• **Specific –** a general consent to share information with 'partner organisations' would not be valid. Specific means that individuals are aware of what particular information will be shared, with whom and for what purpose.
• **A positive indication by the data subject -** the provision of opt outs on forms is not sufficient to obtain the consent of an individual.
• **Freely given** - the individual is not acting under duress from any party.

In practice, the treatment of confidential information needs to be based on the following considerations:
• The child, young person and/or their parent/carer should be told about the partner's confidentiality policy at the beginning of involvement and about routine information sharing between partners for purposes of consultation and supervision, and between statutory agencies when there are legal requirements.
• It is good practice to ask parent/carers or the young person to sign an agreement giving consent to the envisaged sharing of information
• The young person or the parent/carer should also be told that if he reveals that he, or another young person, is at risk of suffering significant harm or has information that will lead to prevention/detection of a serious crime, this information will be disclosed to children's services or the police.

In relation to children and young people (unless the young person is deemed to be

Gillick competent, which relates to a young person under 16 deemed able to consent to medical treatment), parental consent should be sought to share information. The practitioner seeking consent must confirm that the adult has parental responsibility. At times, another party may be required to consent on behalf of the parent, for example someone with a power of attorney or able to exercise the court of protection. Only one party with parental responsibility is required to give consent.

Those young people who are Gillick competent can give consent in their own right. Section 66 of the Data Protection Act provides that a person under 16 may exercise any right under the act when he has a general understanding of what it means to exercise that right; and that a person of 12 years or more shall be presumed to be of sufficient age and maturity to have such understanding.

When obtaining consent to pass on or seek information from another agency, an explanation must be given to the service user about:

- The purpose of approaching other individuals or agencies
- The reason for disclosure of information
- Details of the individuals or agencies being contacted
- What information will be sought and shared
- Why the information is important
- What it is hoped will be achieved

Wherever possible, and certainly where young people are deemed to be Gillick competent, children and young people should be directly included in these explanations. Consent should be obtained in writing. If this is not possible, a practitioner should note the circumstances in which consent was sought and gained.

6.2 Sharing information without consent

If the person with parental responsibility or a young person of Gillick competence wants information about them withheld from someone or some agency which might otherwise have received it, the individual's wishes must be respected unless there are exceptional circumstances.
Examples of circumstances in which a service user's or their parent's/carer's right may be overridden may include where:

- Information is required by statute or court order
- There is a serious risk to individual or public health if the information is not

shared

- There is a risk of harm to the individual and/or other individuals (including children)
- The sharing of the information is necessary for the prevention, detection or prosecution of crime

The decision to disclose must have regard to any duty of confidentiality and the individual's human rights. Every effort, however, must be made to explain to the individual the consequences of their refusal to consent to the disclosure of the information, but the final decision rests with the individual.

Where it is necessary to share information without consent, it is important that the information is shared only with those who 'need to know' and is limited to such information that is essential to fulfil the purpose of the disclosure, such as to protect a child from significant harm.

Where disclosure of a child's information might reveal information about other individuals, such as parents or other family members, explicit consent should be sought from these individuals as well.

If information is disclosed without consent, full details should be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed.

A record of the disclosure should be made in the service user's case record and they must be informed if they have the capacity to understand or, if they do not, a person with parental responsibility must be informed unless to do so would be or would likely to be harmful to the service user or any other person, would interfere with a criminal investigation or other exceptional circumstances.

Where it is not practicable to seek consent or where the individual is not competent to give consent, it is important to consider whether disclosure would be justified in the public interest such as to protect others from a risk so serious that it outweighs the individual's right to privacy. This needs consideration in collaboration with the appropriate Caldicott guardian/ equivalent.

Recipients of the information must be made aware that it has been disclosed without consent and will put agreed security procedures in place. The recipient of information should record the details of the information received, who provided the information, any restrictions placed on the information that has been given such as 'not to be disclosed to the service user', that the information was provided without consent, and the reason.

6.3 Recording consent

Although it is not a legal requirement to have obtained written or signed consent, it is always advisable to keep a record of when an individual's consent has been obtained as evidence to confirm that information has been made available to them.

Agencies should store the consent form appropriately, for example the service user's personal file. The file should be marked to indicate that consent forms are present. A copy of the consent form should be made available to the service user or any person acting on their behalf.

If a service user or any person acting on their behalf requests that the disclosure of the information should be limited to specific agencies/persons, agencies must ensure that this is made clear on the consent form and on the agency records to ensure that members of staff are alerted to the limits of the consent. This limitation of consent should be recorded whether or not a decision is taken to disclose any information without consent.

If the service user or their parent/carer withdraws consent at any time, a record must be kept of the date on which their initial consent was given, the date on which it was due to expire and the date on which it was withdrawn. If at any time following the withdrawal or expiry of consent, a partner wishes to disclose that information for the same or another purpose, then consent will again need to be sought from the service user and/or parent/carer.

6.4 Data subject access requests

General rights

Individuals have the right to see the information held about them whether it is held in electronic or manual files. All subject access requests must be passed to an authorised person, as described in the partner agencies data protection policy and procedures. All requests must be dealt with within 40 working days of receipt of the request.

Information belonging to another agency

If an agency receives a request from the data subject to have access to their personal data and this information is identified as belonging to another agency, the receiving agency must contact the originating agency to determine whether they wish to claim an exemption under the provisions of the Data Protection Act.

Information which discloses the identity of a third party

Where a data controller cannot comply with the request without disclosing information relating to another individual, who can be identified from that information, he is not obliged to comply with the request unless:

- The other individual has consented to the disclosure of the information to the person making the request
- It is reasonable in all the circumstances to comply with the request without the consent of the individual.
- In determining whether it is reasonable, regard shall be had to all the circumstances but in particular to:
    - Any duty of confidentiality owed by or to the other individual
    - Any steps taken by the data controller with a view to seeking the consent of the other individual
    - Whether the other individual is capable of giving consent
    - Any express refusal of consent by the other individual

Information held jointly

In the case of joint records, either agency can provide access to the joint record, provided the individual is informed that the information is held jointly. Where there are joint holding arrangements, agencies need to ensure that they have procedures in place to enable the individual to be made aware that he is not obliged to apply to all of the agencies for access and to ensure that each agency is informed that access has been given.

7. Protocol operation

Dissemination and circulation of the framework

Partners must ensure that the framework is published on their website and made available at appropriate information points. Partners must ensure that copies of framework are made available to all relevant staff, in line with each partner's internal arrangements. Wherever possible, the framework should also be available to staff online.

Other protocols

Where other protocols already exist between agencies, this framework and associated local procedures will run concurrently with them. Statutory guidance on information sharing will take precedence over this framework.

Further protocols may be required to support joint working in relation to specific service areas or initiatives relating to services for children, young people and their families.

Agents and sub-contractors

Each partner shall ensure its agents and sub-contractors comply with the provisions of this framework.

Nominated representatives

Each partner organisation shall have a nominated representative for the purpose of this code of practice to perform management functions in relation to the sharing of personal information. This could be your data protection officer or Caldicott Guardian.

Monitoring arrangements

Partner organisations will take lead responsibility for monitoring and reviewing the implementation of the protocol. The Protocol will be formally reviewed by the SSCB within a year of issue.

Reviewing arrangements

This framework will be subject to regular review, following any changes in statutory guidance or at least every year. Each partner should have an allocated person to respond to queries regarding the framework and monitor its operation.

Staff compliance

Each partner will ensure that all staff who work with client information are fully trained and understand and comply with their responsibilities to share information in accordance with agreed protocols. Partner organisations will ensure that all staff are made aware of their obligations under the Data Protection Act 1998, their duty of care and confidentiality.

Codes of conduct

Each partner will ensure that job descriptions make reference to the principles of confidentiality and data protection, codes of conduct and disciplinary action which will be taken should staff disclose information about a person on a basis that is not supported in agreed protocols. Partner organisations will ensure that staff found in breach of policies and procedures, are investigated accordingly.

Complaints

Where parents, children or young people consider their confidentiality has been breached they have a right to complain via the internal complaints procedure of the partner alleged to have breached the confidence. This will not affect their additional rights of redress as detailed in the Data Protection Act. In the event of a complaint being received by any partner included in this framework about the use or disclosure of personal information, all relevant partners must be advised as soon as practicably possible and in any event within seven working days. Each partner will deal with the complaint in accordance with their own procedures, the results of which will be advised to all other partners and any necessary action to amend the framework will be taken.

Indemnity

Disclosure of personal or sensitive information without consent must be justifiable on statutory grounds or meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both the partner and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.

Where a disclosing partner provides information to a requesting agency, both parties are entitled to assume that both the request and the disclosure are compliant with the requirements of the Data Protection Act.

Where a disclosing agency provides information to a requesting agency that is inaccurate, and the requesting agency incurs liability, cost or expense as a result of its reliance on the

information provided, the disclosing agency shall indemnify the requesting agency against any such liability, cost or expense reasonably incurred, provided that this indemnity shall not apply:

- Where the disclosing agency did not know, and acting reasonably, had no reason to know, that the information provided was inaccurate
- Unless the requesting agency notifies the disclosing agency as soon as practicable of any action, claim or demand to which it considers this indemnity may apply, permits the disclosing agency to deal with the action, claim or demand by settlement or otherwise and renders all reasonable assistance in so doing

8. Declaration of acceptance

Agreement: We the undersigned do hereby agree to:

- implement and adhere to the terms and conditions of this protocol
- Ensure that all operational procedures established between agencies for the purposes of information sharing are consistent with this framework.

Name	**Signature**

9. References

For further information, refer to the below:

The Data Protection Act

http://www.ico.gov.uk/for_organisations/data_protection.aspx

Information sharing – advice for practitioners providing safeguarding services to children, young people, parents and carers HM Government March 2015

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419628/Information_sharing_advice_safeguarding_practitioners.pdf

Working Together 2015

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419595/Working_Together_to_Safeguard_Children.pdf

Children Act 2004

http://www.legislation.gov.uk/ukpga/2004/31/contents

APPENDIX 1

The Legal Framework

Legislation under which most public sector agencies operate, defines the role, responsibility and power of the agency to enable it to carry out a particular function. There is no general power to disclose data and there is no general power to obtain, hold or process data. The legislation referred to below may not be relevant to all partner organisations. Partner organisations must ensure they are acting lawfully.

The Data Protection Act 1998

The Act governs the processing of information relating to individuals, including obtaining, holding, use or disclosure of such information.

Personal data means data relating to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual..

Any organisation who determines the purposes for which and the manner in which any personal data are, or are to be processed (obtaining, recording, holding, using, disclosing and disposing) is a 'Data Controller' responsible for abiding by the 8 data protection principles and notifying the Information Commissioner of that processing.

The Act gives seven rights to individuals in respect of their own personal data held by others:

1. The right to access their own information (subject access request);
2. right to prevent processing likely to cause damage or distress;
3. The right to prevent processing for the purposes of direct marketing;
4. Rights in relation to automated decision taking;
5. The right to take action for compensation if the individual suffers damage or damage and distress (as a result of any breach of the act);

6. The right to take action to rectify, block, erase or destroy inaccurate data;
7. The right to request the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

The 8 key principles of the Act are:

Principle 1	Personal data shall be processed fairly and lawfully and shall not be processed unless at least 1 of the conditions in Schedule 2 is met and for 'sensitive personal data' at least 1 of the conditions in Schedule 3 is also met.
Principle 2	Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose/purposes.
Principle 3	Personal data shall be adequate, relevant and not excessive in relation to the purpose/purposes for which they are processed.
Principle 4	Personal Data shall be accurate and, where necessary kept up to date
Principle 5	Personal data shall not be kept for longer than is necessary for that purpose/purposes.
Principle 6	Personal data shall be processed in accordance with the rights of the data subject under this Act.
Principle 7	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.
Principle 8	Personal data shall not be transferred to a country or territory outside the European Economic Area without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

The Human Rights Act 1998

The Human Rights Act 1998 incorporates into our domestic law certain articles of the European Convention on Human Rights (ECHR). The Act places a legal obligation on all Public Authorities to act in a manner compatible with the Convention. Should a Public Authority act inconsistently then it may be the subject of legal action. The sharing of information between agencies has the potential to infringe Article 8.1 in particular.

Article 8.1 provides that "everyone has the right to respect for his private and family life, his home and his correspondence". This right may be only

breached by a public authority if the breach is in accordance with the law and is necessary in the interest of one of the following legitimate aims: national security, public safety or the economic well-being of the country for the prevention of crime and disorder, for the protection of health and morals or for the protection of the rights and freedoms of others.

The following factors should be taken into account when deciding whether disclosure of information would breach a person's right to privacy:

- Is there a legal basis for the action being taken?
- Does it pursue a legitimate aim?
- Is the action taken proportionate and the least intrusive method of achieving that aim?

The Freedom of Information Act (FOIA) 2000

The Freedom of Information Act (FOIA) gives a general right of access to the public of all types of recorded information held by defined public authorities from 1 January 2005.

There are 23 statutory exemptions to the right of access which are either absolute or qualified. Absolute exemptions include personal information if disclosure would breach the data protection principles. Qualified exemptions require the public authority to consider first whether or not the exemption applies, on a case-by-case basis. Secondly, if the exemption does apply, the public authority must then consider whether it is in the public interest to apply the exemption. Further information and guidance can be found at the following web site http://www.ico.gov.uk

The Common Law Duty of Confidentiality

There is a common law duty of confidentiality which must be adhered to:

'In Confidence'… Information is said to have been provided in confidence when it is reasonable to assume that the provider of that information believed that this would be the case, in particular were a professional relationship may exist e.g. doctor/patient, social worker/client; lawyer/client etc.

The duty of confidentiality requires that unless there is a statutory requirement or other legal reason to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g. to protect others from harm).

Caldicott Principles

The Caldicott Committee carried out a review of the use of patient-identifiable information. It recommended a series of principles that should be applied when considering whether confidential information should be shared. All NHS organisations and Social Services Departments are now required to apply the Caldicott principles. These principles relate to the use of patient-identifiable information and are detailed below.

Principle 1	Justify the purpose for using such information. Every proposed use or transfer of such information should be clearly defined and scrutinised and continuing uses reviewed regularly.
Principle 2	Only use such information when absolutely necessary.
Principle 3	Use the minimum amount of personal information that is required for a given function to be carried out
Principle 4	Access to personal information should be on a strict “need to know” basis. Only those staff who need such information in order to carry out their roles should have access and this should be limited to specifically relevant information.
Principle 5	Everyone with access to such personal information needs to be aware of their responsibilities and their obligations in respect of confidentiality.
Principle 6	Understand and comply with the law. Someone in each organisation that handles personally identifiable information should be responsible for ensuring that the organisation complies with legal requirements
Principle 7	The duty to share can be as important as the duty to protect confidentiality

All Health and Social Services organisations are required to nominate a senior person to act as a Caldicott Guardian responsible for safeguarding the confidentiality of patient information.

Examples of Statutory Gateways for disclosure

There are many examples of legal gateways which allow disclosure. Some examples are listed below:

Crime and Disorder Act 1998

The Act introduced measures to reduce crime and disorder. Section 115 provides that any person has the power to lawfully disclose information to the police, local authority, probation service or health authority (or persons acting on their behalf) where they do not otherwise have the power, but only where the disclosure is necessary or expedient for the purposes of any provision of the Act.

However, whilst all agencies have the power to disclose, Section 115 does not impose a requirement on them to exchange information and does not override the need to disclose in a proper manner taking into account Data Protection Principles and Article 8 Human Rights Convention.

Local Government Act 2000

Under Section 2 local authorities may do anything, which they consider likely to achieve any one or more of the following objects:

- the promotion or improvement of the economic well-being in their area;
- the promotion or improvement of the social well-being of their area; and
- the promotion or improvement of the environmental well-being of their area.

The power may not be exercised where there is an express restriction on doing so.

National Health Service and Community Care Act 1990

Under Section 47 When a local authority is assessing need and it appears that there may be a need for health or housing provision, the local authority shall notify the appropriate primary care trust or local housing authority and invite them to assist to such extent as is reasonable in the circumstances in the making of the assessment.

Children Act 1989

Sections 27 and 47 of the Children Act 1989 enable local authorities to request help from specified authorities (other local authorities, education authorities, housing authorities, NHS bodies) and place an obligation on those authorities to co-operate. A request could be for information in connection with a section 17 needs assessment or a section 47 child protection enquiry.

Children Act 2004

The Children Act 2004 created the legislative framework for developing more effective and accessible services focused around the needs of children, young people and families by ensuring co-operation, clearer accountability and safeguarding of children.

2BSection 10 (co-operation to improve well-being) Section 10 establishes a duty on Local Authorities to make arrangements to promote co-operation between agencies in order to improve children's well-being, defined by reference to the five outcomes and a duty on key partners to take part in those arrangements. It also provides a new power to allow pooling of resources in support of these arrangements.

3BSection 11 (arrangements to safeguard and promote welfare) brings with them an implied duty to share information when judged to be in the best interests of the child. That is, those bodies bound by the duties should share information about children as part of furthering those duties. The Children Act 2004, therefore, adds to and reinforces the existing body of legislation that gives (usually in an implied way) legal foundation to information sharing when the interests of a child require it.

In addition section 14B of the Children Act 2004 outlines guidance re the supply of information requested by LSCB's:

(1) If a Local Safeguarding Children Board established under section 13 requests a person or body to supply information specified in the request to—
(a) the Board, or
(b) another person or body specified in the request,
the request must be complied with if the first and second conditions are met and either the third or the fourth condition is met.

(2) The first condition is that the request is made for the purpose of enabling or assisting the Board to perform its functions.

(3) The second condition is that the request is made to a person or body whose functions or activities are considered by the Board to be such that the person or body is likely to have information relevant to the exercise of a function by the Board.

(4) The third condition is that the information relates to—
(a) the person or body to whom the request is made,
(b) a function or activity of that person or body, or
(c) a person in respect of whom a function is exercisable, or an activity is engaged in, by that person or body.

(5) The fourth condition is that the information
(a) is information requested by the Board from a person or body to whom information was supplied in compliance with another request under this section, and
(b) is the same as, or is derived from, information so supplied.

(6) The information may be used by the Board, or other person or body to whom it is supplied under subsection (1), only for the purpose of enabling or assisting the Board to perform its functions.
(7) A Local Safeguarding Children Board must have regard to any guidance given to it by the Secretary of State in connection with the exercise of its functions under this section.

Education Act 2002

S175 (2) provides that the governing body of a maintained school shall make arrangements for ensuring that their functions relating to the conduct of the school are exercised with a view to safeguarding and promoting the welfare of children who are pupils at the school.

Examples of statutory restrictions to information sharing

NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000 prevent the disclosure of any identifying information about a patient with a venereal disease other than to a medical practitioner under specified circumstances.

The Human Fertilisation and Embryology Act 1990 (as amended) limits the circumstances in which information may be disclosed by centres licensed under the Act.

The Abortion Regulations 1991 limit and define the circumstances in which information submitted under the Act may be disclosed.

IF IT SEEMS LIKELY THAT INFORMATION TO BE SHARED FALLS INTO ONE OF THESE CATEGORIES FURTHER ADVICE SHOULD BE SOUGHT.