

Merton Safeguarding Children Board

Information Sharing Protocol



March 2017

Author: Paul Bailey Lead:	Date Updated: March 2017	Approved By MSCB: January 2015	Review Date: TBC
---	------------------------------------	--	----------------------------

1. Who does the Information Sharing Protocol affect?	3
2. The benefits of this Information Sharing Protocol.....	3
3. Principles of Information Sharing.....	3
4. Obtaining and sharing information.....	3
5. Confidential information.....	4
6. Obtaining consent	5
7. Sharing Information Appropriately and Securely	6
8. Retaining and storing Information.....	6
9. Regular review	6
10. Flowchart for Information Sharing	7
11. Signatories to the Protocol	8
12. Information Sharing Checklist	10
13. Legislation/Guidance.....	10
14. Seven golden rules for Information Sharing, HM Government:.....	11
15. The Caldicott Principles	11

1. Who does the Information Sharing Protocol affect?

The protocol affects all staff engaged with work involving children and families (including parents known to adult services) that requires information to be shared with, or is given to them by other organisations.

2. The benefits of this Information Sharing Protocol

- Help remove barriers to effective information sharing.
- Provide guidance to assist in complying with legislation.
- Help to ensure that consent to share personal information is obtained whenever it is required.
- Help to ensure that information is shared when there is a requirement to do so.
- Help to ensure that all agencies comply with relevant legislation.
- Raise awareness amongst all agencies of the key issues relating to information sharing and give confidence in the process of sharing information with others.

3. Principles of Information Sharing

Effective information sharing underpins integrated working and is a vital element of both early intervention and safeguarding. Each partner can hold different pieces of information which need to be placed together to enable a thorough assessment to be made.

To share information about a person you need a clear and legitimate purpose to do so, as this will determine whether the information sharing is lawful. For partners working in statutory services, the sharing of information must be included within the powers of the service. This will also apply if partners from the voluntary sector are contracted to provide a service on behalf of a statutory body.

Sharing of information will comply with the Caldicott Principles.

4. Obtaining and sharing information

The sharing of information must have due consideration with the law relating to confidentiality, data protection and human rights. Having a legitimate purpose for sharing information is an important part of meeting

those legal requirements. It is important only to share as much information as is needed and records should be accurate, relevant and up to date.

5. Confidential information

Confidential information is:

- Private or sensitive personal information.
- Information which is not already lawfully in the public domain or readily available from another public source.
- Information that has been provided in circumstances where the person giving the information could reasonably expect that it would not be shared with others.

This is a complex area and you should seek advice from your organisation's Information Manger, if you are unsure about confidentiality

Signatory agencies to this protocol may lawfully share confidential information without obtaining consent only if this an overriding public interest. Judgement is required on whether there is sufficient public interest using the facts of each case individually. Public interest can arise when protecting children from significant harm, promoting the welfare of children or preventing crime and disorder.

Proportionality and necessity are factors to be taken into consideration when deciding whether or not to share confidential information. In making the decision, practitioners must weigh up what might happen as a result of the information being shared against what might happen if it is not and apply their professional judgement.

The nature of the information to be shared is also significant where the information is sensitive and has implications for the practitioner's relationship with the individual, recognising the importance of sharing information in a timely manner if it is in the child best interest to do so.

Where there is a clear risk of significant harm to a child you must share the information to safeguard the child

6. Obtaining consent

Consent must be informed, in other words the person giving consent needs to understand:

- Why the information needs to be shared
- Who will see it
- How much will be shared
- What are the purposes and implications of sharing

It is good practice for signatories to set out their policy on sharing information when clients first join a service and when securing information, the process should be transparent and respect the individual. Consent must not be obtained by coercion and must be sought again if there are to be significant changes in the use to be made of the information.

A child or young person, who is able to understand and make their own decisions, may give or refuse consent to share information. This would generally include children aged over 12, although younger children may have sufficient understanding. The child's view should be sought as far as possible. If a child is competent to give consent or refusal but a parent disagrees each individual case should be considered and again professional judgement should be applied and documented.

When assessing a child's ability to understand, practitioners should explain in a way suited to their age, language and likely understanding. Where a child cannot consent, a person with parental responsibility should be asked to do so, on their behalf, although there are circumstances where this might be inadvisable. Where parenting is shared only one person with parental responsibility for a child needs to give consent.

In some cases it may not be appropriate to let a person know that information about them is being shared nor to seek their consent to share the information. For example, this would arise when sharing information is likely to hamper the prevention or investigation of a serious crime or put a child (or adult) at risk of significant harm.

In these circumstances, practitioners need not seek consent from the person or their family nor inform them that the information will be shared; but should record their reasons for sharing information without consent or informing the person about whom the consent is being shared. .

Similarly, consent need not be sought when practitioners are required to share information through a statutory duty or court order. However, in most circumstances they should inform the person concerned that they are sharing the information, why they are doing so and with whom.

7. Sharing Information Appropriately and Securely

Information should be shared in accordance with the principles of the Data Protection Act 1998 and follow the policy and procedures of the signatory service.

Information should always be shared safely, either by secure IT connection, secure email or secure transfer of paper documents. Information should never be sent via a non secure method.

Practitioners should:

- Only share the information which is necessary for the purpose.
- Understand the limits of any consent given, particularly if it is from a third party.
- Distinguish between fact and opinion.
- Only share it with the person or people who need to know and check that the information is accurate and up to date.
- Record decisions on sharing information and the reasons for doing so or not.
- If deciding to share the information, record what was shared and with whom.
- If deciding to not share the information, record the reasons for this decision.

8. Retaining and storing Information

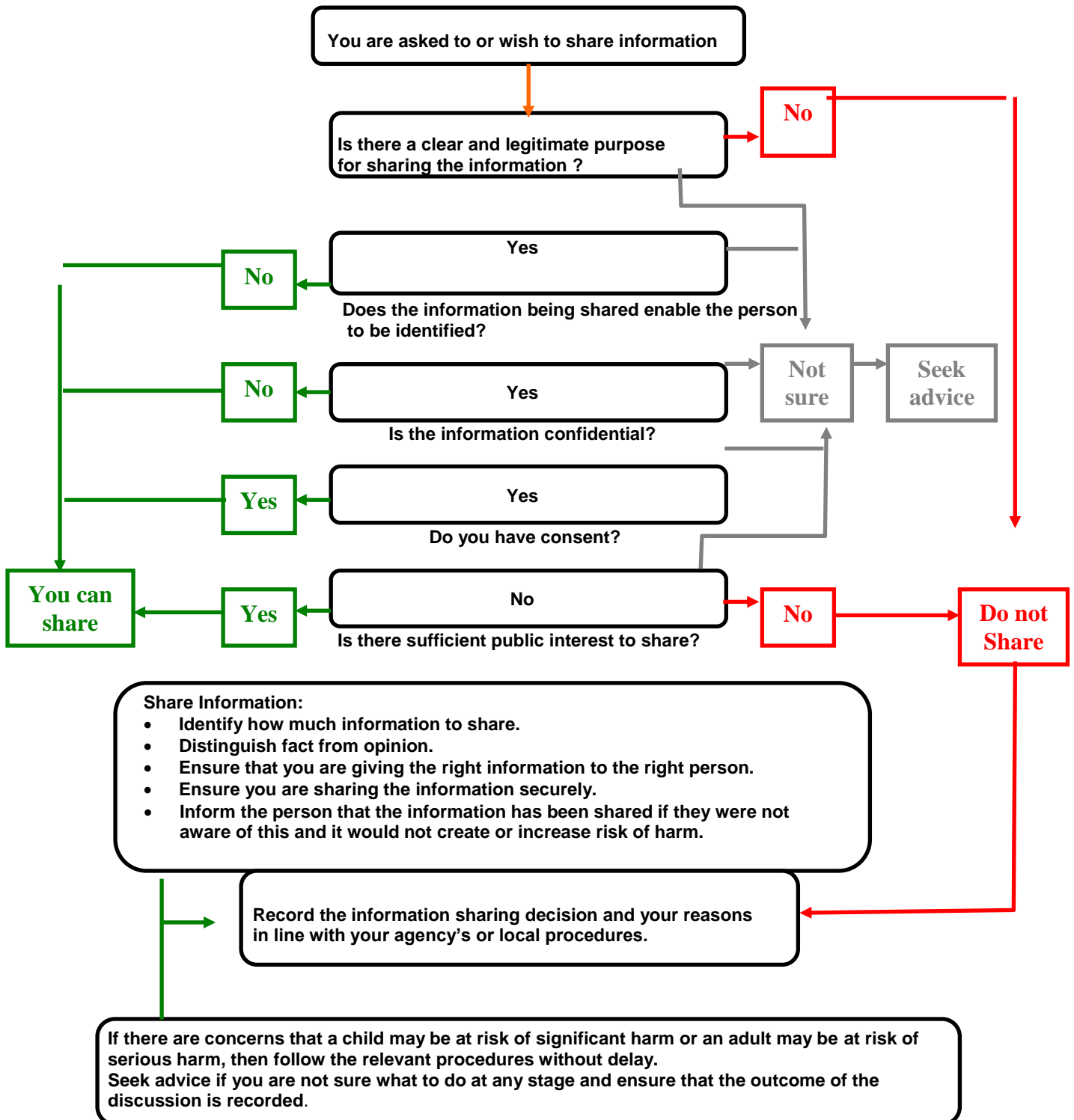
Information must not be retained for longer than necessary for the purpose for which it was obtained. Signatory services should ensure that they have physical and electronic security in place for the stored data and that there is awareness, training and management of the systems where the information is stored.

9. Regular review

This agreement will be reviewed bi-ennially by the Policy Subgroup of the MSCB and amended, as required before that to take account of changes in law, guidance and lessons learned from sharing data.

10. Flowchart for Information Sharing

Flowchart of key questions for information sharing



12. Information Sharing Checklist

- Do I already have informed consent to share this information?
- Is the information sensitive and personal?
- Do I need consent to share the information?
- Have I a legal duty or power to share the information?
- Whose consent is needed?
- Whose information is this?
- Would seeking consent place someone at risk, prejudice a Police investigation, or lead to unjustifiable delay?
- Would sharing the information without consent cause more harm than not sharing the information?
- How much information is it necessary to share in this situation?
- Am I giving this information to the right person?
- Am I sharing this information in a secure way?
- Does the person I am giving it to know that it is confidential?
- What will they do with it?
- Is the service user aware that the information is being shared (where this would not place someone at risk or prejudice a Police investigation)?
- Have I distinguished between fact and opinion?
- Does the person who is giving consent understand the possible consequences of sharing the information?

13. Legislation/Guidance

The Data Protection Act 1998

The Human Rights Act 2000

The Children Act 2004

The Crime & Disorder Act 1998

Freedom of Information Act 2000

NHS Act 2006

Working Together to Safeguard Children 2015

14. Seven golden rules for Information Sharing, HM Government:

- 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 well-being:** Base your information sharing decisions on considerations of the safety and well-being 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.

15. The Caldicott Principles

- 1. Justify the purpose(s)**
Every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.
- 2. Don't use patient identifiable information unless it is absolutely necessary**
Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients

to be identified should be considered at each stage of satisfying the purpose(s).

- 3. Use the minimum necessary patient-identifiable information**
Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
- 4. Access to patient identifiable information should be on a strict need-to-know basis**
Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
- 5. Everyone with access to patient identifiable information should be aware of their responsibilities**
Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
- 6. Understand and comply with the law**
Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.
- 7. The duty to share information can be as important as the duty to protect patient confidentiality**