



# Bromley Multi Agency Children's Safeguarding Information Sharing Protocol



Version	4.0
Ratified	01/03/2017
Next Revision	April 2020

## Contents:

1. Introduction	3
2. Who does this information sharing protocol affect?	4
3. The benefits of the information sharing protocol	4
4. Principles of Information Sharing	4
5. Legal basis for information sharing	6
6. Confidential information	6
7. Obtaining consent	7
8. Sharing information appropriately and securely	8
9. Retaining and storing information	9
10. Regular review	9
11. Escalation policy	9
12. Signatories	9
Appendix – Information sharing flowchart and checklist	10-11

## 1. Introduction

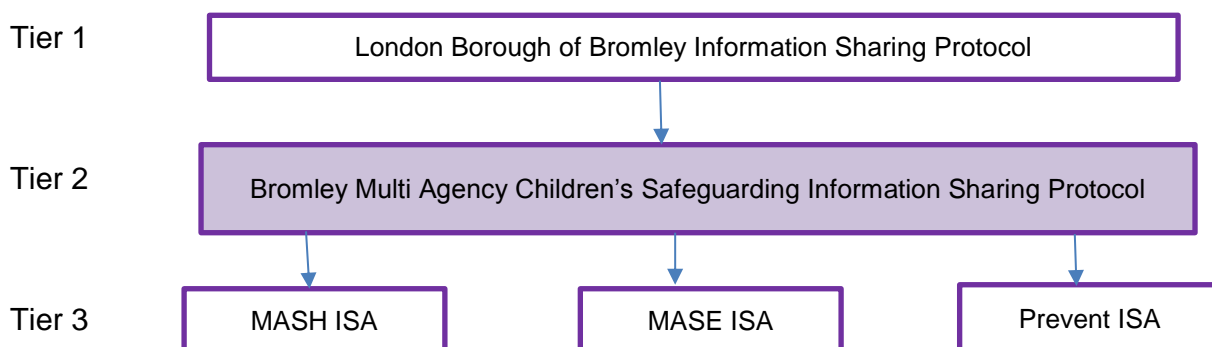
This guidance is written primarily to support professionals to understand what information they can share legally and in the best interests of the child. The best outcomes for children and young people, including keeping them safe, comes from good multiagency working and communication.

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

Bromley Safeguarding Children Board is made up of statutory and voluntary partners, representatives from Health, Children's Services, Police, Probation, the Community and Voluntary Sector as well as Lay Members. Our main role is to coordinate what is done locally to protect and promote the welfare of children and young people in Bromley and to monitor the effectiveness of those arrangements to ensure better outcomes for children and young people.

There is an overarching Bromley Strategic Partnership Information Sharing Protocol (Tier 1) that covers the high level principles that all partner organisations, for both adults and children, sign up to within the borough. This Bromley Multi Agency Children's Safeguarding Information Sharing Protocol (ISP) sits beneath this (Tier 2) and focusses on safeguarding. At the next level, there are Individual Service Agreements (ISAs) for information sharing such as MASH (Multi Agency Safeguarding Hub), MASE (Multi Agency Safeguarding Panel for Sexual Exploitation) and Prevent.

Professionals working with children and young people should refer to this Tier 2 ISP for guidance on sharing relevant information proportionately to safeguard the child.

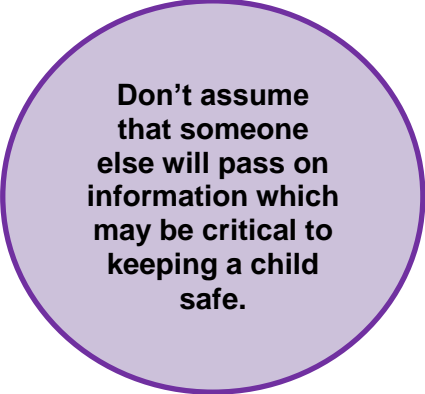


## 2. Who does the Information Sharing Protocol Affect?

This 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 that is given to them, by other organisations.

## 3. 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.
- Raise awareness amongst all agencies of the key issues relating to information sharing and give confidence in the process of sharing information with others.



**Don't assume that someone else will pass on information which may be critical to keeping a child safe.**

## 4. 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 and the 7 Golden Rules to Sharing Information](#) (see page 5).

## The 7 Golden Rules to Sharing Information

1. The Data Protection Act 1998 and human rights law are **not barriers** to justified information sharing. They provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be **open and honest** with the individual (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 if you are in any **doubt** about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Share with **informed 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, there is good reason to do so, such as where **safety may be at risk**. Base your judgement on the facts.
5. Consider safety and well-being: **Base your information sharing decisions on considerations of the safety and well-being** of the individual and others who may be affected by their actions.
6. **Necessary, proportionate, relevant, adequate, accurate, timely and secure:** Ensure that 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 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.

## The 7 Caldicott Principles:

1. **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, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use personal confidential data unless it is absolutely necessary** Personal confidential data 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 personal confidential data** Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out
4. **Access to personal confidential data should be on a strict need-to-know basis** Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes
5. **Everyone with access to personal confidential data should be aware of their responsibilities** Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.
6. **Comply with the law** Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
7. **The duty to share information can be as important as the duty to protect patient confidentiality** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

## 5. Legal basis for information sharing within this guidance

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 proportionate information as is needed and records should be accurate, relevant and up to date.


The key legislation and guidance affecting the sharing and disclosure of data includes (this is not necessarily an exhaustive list):

- [The Mental Health Act 1983](#)
- [The Access to Health Records Act 1990](#)
- [The Data Protection Act 1998](#)
- [The Human Rights Act 1998](#)
- [The Local Government Act 2000](#)
- [The Education Act 2002](#)
- [The Freedom of Information Act 2000](#)
- [The Criminal Justice Act 2003](#)
- [The Children Act 2004](#)
- [The Mental Capacity Act 2005](#)
- [The Health and Social Care Act 2012](#)
- [The Common Law Duty of Confidentiality](#)
- [The Crime and Disorder Act 1998](#)
- [FGM Mandatory Guidance](#)
- [Department for Education Information Sharing for Practitioners](#) March 2015
- [Working Together to Safeguard Children 2015](#)
- [London Child Protection Procedures 2016](#)
- [NHSE Safeguarding Vulnerable People in the NHS – Accountability and Assurance Framework 2015](#)

## 6. 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.



**The most important consideration is whether sharing information is likely to safeguard and protect a child**

**This is a complex area and you should seek advice from your organisation's Information Manager and/or Caldicott Guardian, if you are unsure about confidentiality**

Signatory agencies to this protocol may lawfully share confidential information without obtaining consent only if there is 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.

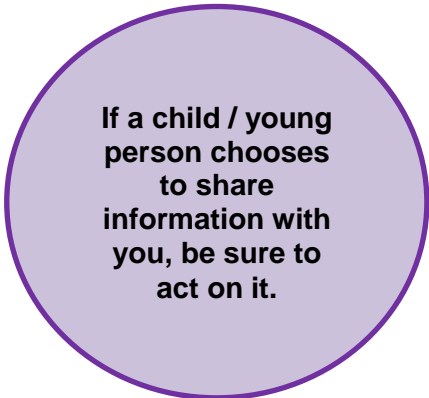
Although sharing of information can impact on a practitioner's relationship with an individual/family, keeping the child safe must be the first consideration. **Where there is a clear risk of significant harm to a child you must share the information to safeguard the child.**

## 7. 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/have access to it
- How much information 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, respect the individual and also ensure that the individual understands when and how their information will be shared. 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.



**If a child / young person chooses to share information with you, be sure to act on it.**

### **Gillick Competency and Fraser Guidelines:**

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. Consideration should be given to the child's emotional age, particularly if they have suffered abuse or trauma. [The Gillick competency and Fraser guidelines](#) help to balance children's rights and wishes with our responsibility to keep children safe from harm.

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.

### **When Consent is Not Required**

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.

**No review into multi agency working has ever criticised practitioners for sharing too much information regarding child protection concerns. The reverse is the case, often with potentially devastating consequences for the child, but also for the practitioner.**

## **8. 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. Secure emails for local authority, health and police follow this format:

Jane.Smith@bromley.gcsx.gov.uk

Jane.smith@nhs.net

Jane.Smith@met.pnn.police.uk

### **Practitioners should:**

- Only proportionately 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.

## **9. 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. Please refer to your own organisation's storage policy.

#### **10. Regular Review**

This agreement will be reviewed every two years by the BSCB Policy and Procedures Subgroup or as required before that to take account of changes in law, guidance and lessons learned from sharing data.

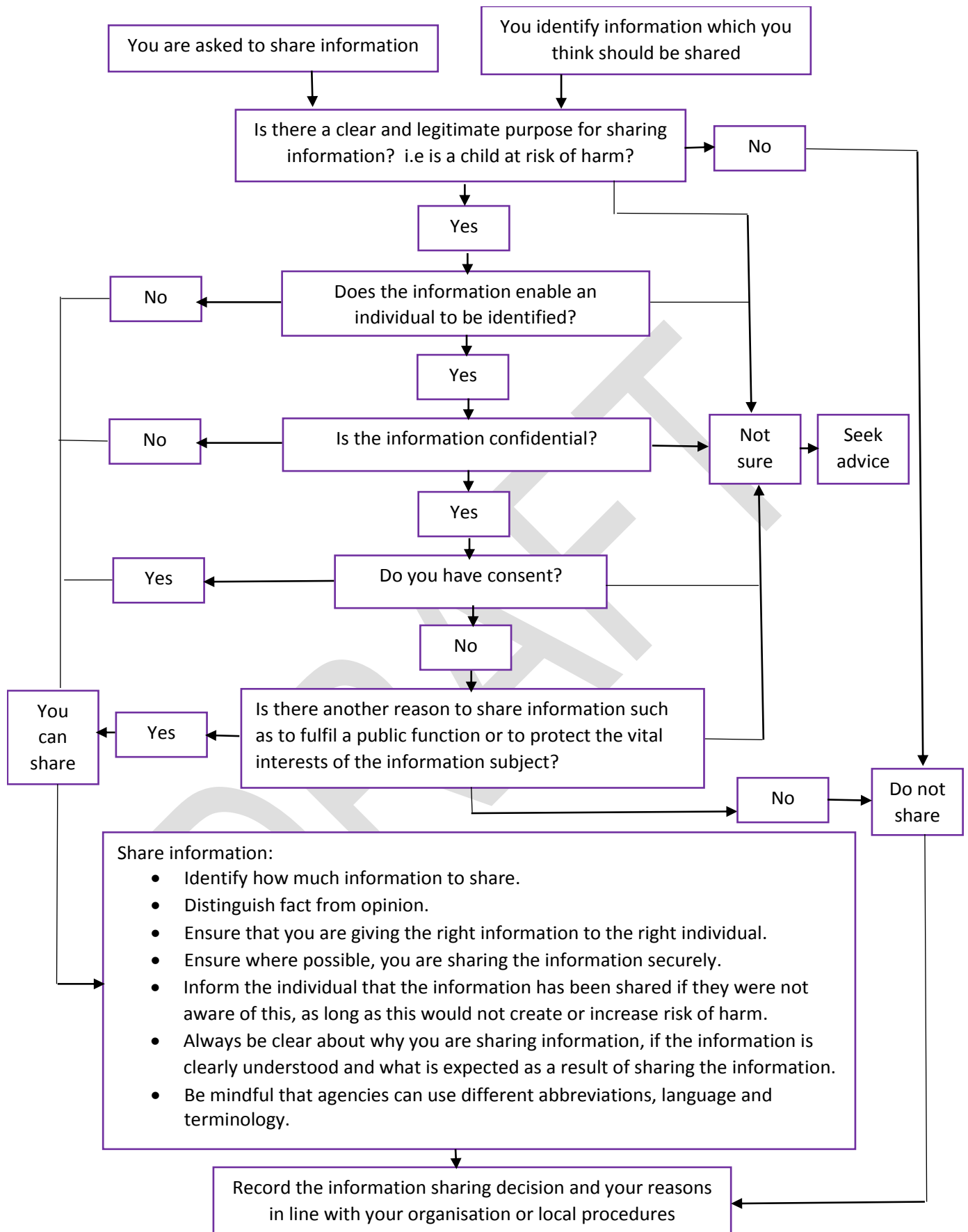
#### **11. Escalation Policy**

Generally there is a good working relationship between agencies, but occasionally there will be a difference of professional views. Staff across all partner agencies are reminded of the Bromley Safeguarding Children Board's Escalation Policy. The aim of this document is to inform the quick resolution of cases where a child or young person may be at risk of significant harm and agencies cannot agree a way forward.

#### **12. Ratification**

This protocol is provided to meet the needs of partners and it is intended that all partners will use the protocol. Board partners ratified this protocol on 1<sup>st</sup> March 2017.

## Appendix: Information Sharing Flowchart and Checklist



If there are concerns that a child is suffering or likely to suffer harm then follow the relevant procedures without delay. Seek advice if unsure what to do at any stage and ensure that the outcome of the discussion is recorded.

## Appendix: Information Sharing Flowchart and Checklist

### 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?

### What do Rules 6 and Rule 7 of the Golden Rules mean?

**Necessary and proportionate:** When taking decisions about what information to share, you should consider how much information you need to release. The Data Protection Act 1998 requires you to consider the impact of disclosing information on the information subject and any third parties. Any information shared must be proportionate to the need and level of risk.

**Relevant :** Only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make sound decisions.

**Adequate:** Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

**Accurate:** 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.

**Timely:** Information should be shared in a timely fashion to reduce the risk of harm. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore harm to a child.

**Secure:** Wherever possible, information should be shared in an appropriate, secure way. You must always follow your organisation's policy on security for handling personal information.

**Record:** Information sharing decisions should be recorded whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with each organisation's own retention policy, the information should not be kept any longer than is necessary. In some circumstances this may be indefinitely, but if this is the case there should be a review process.