Manchester Settlement
widening horizons since 1895

Information Sharing and Confidentiality Policy

Policy Status:	Statutory
Review Cycle:	2
Policy Reference:	

Review Date	Author	Change History
01/02/16	AB	New Policy Combining IS and Confidentiality to take account of DfE guidance
01/02/18		

1. Contents

1. Contents 1
2. Introduction 2
3. Aims of the Policy 2
4. Legal context 3
5. Scope 3
6. Sharing Information 3
7. When and how to share information 4
8. The Seven Golden Rules to Sharing Information 5
9. Flowchart of When and How to Share Information 6
10. Confidentiality Principles 6
11. Staff responsibilities 7
12. Contractual Obligations 8
13. Resources 8

2. Introduction

This policy sets out our commitment to

- Sharing Information regarding children, young people and vulnerable adults where necessary to ensure they are safeguarded from harm.
- Maintaining the confidentiality of personal information in the course of providing our services. supporting our commitment to our service users and their families and contributes to our meeting our legislative obligations.

Sharing information is an intrinsic part of any frontline practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. It could ensure that an individual receives the right services at the right time and prevent a need from becoming more acute and difficult to meet. At the other end of the spectrum it could be the difference between life and death. Poor or non-existent information sharing is a factor repeatedly flagged up as an issue in Serious Case Reviews carried out following the death of, or serious injury to, a child. Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. No practitioner should assume that someone else will pass on information which may be critical to keeping a child safe.
Professor Munro's review of child protection concluded the need to move towards a child protection system with less central prescription and interference, where we place greater trust in, and responsibility on, skilled practitioners at the frontline.1 Those skilled practitioners are in the best position to use their professional judgement about when to share information with colleagues working within the same organisation, as well as with those working within other organisations, in order to provide effective early help and to keep children safe from harm.
Lord Laming emphasised that the safety and welfare of children is of paramount importance and highlighted the importance of practitioners feeling confident about when and how information can be legally shared.2 He recommended that all staff in every service, from frontline practitioners to managers in statutory services and the voluntary sector should understand the circumstances in which they may lawfully share information, and that it is in the public interest to prioritise the safety and welfare of children.
Dfe 2015

When a person gives us information in confidence that means they expect us to keep it to ourselves and not to make it generally known or tell others without their permission. A request for confidentiality may be explicit, or there may be an implicit expectation that information is given in confidence. People have a reasonable expectation that personal information they give in the context of our service will be treated confidentially. However the nature of many of our services require a high level of professional intervention to safeguard service users, and information sharing is essential for this

This policy sets out the principles of confidentiality and respect for privacy that staff are expected to understand and follow. It also sets out the safe way that staff can share information.

Staff must use your judgement to apply the principles in the policy and guidance to the situations you face in your own practice. The purpose of the guidance is to help you identify the relevant legal and ethical considerations, and to help you make decisions that respect our customers' privacy, autonomy and choices, and that also benefit the wider community. If in doubt, you should seek the advice of your manager.

3. Aims of the Policy

The aim of the policy is to ensure personal and other confidential information is managed appropriately so that:

- Privacy and confidentiality are respected
- The Data Protection Act and other legal requirements are satisfied
- The public and partner agencies can be confident that we handle personal information appropriately.

4. Legal context

There are many statutory provisions giving duties to protect confidential information, or in some cases to pass it on appropriately. The Data Protection Act 1998, the Human Rights Act 1998 and the common law duty of confidence must all be considered. The Mental Capacity Act 2005 provides a statutory framework for people who may lack capacity to make decisions themselves. The Code of Practice for the Mental Capacity Act (http://www.dca.gov.uk/legal-policy/mental-capacity/mca-cp.pdf) contains guidance (Chapter 16) about access to information about a person who lacks capacity and about when health/social staff may disclose information about someone who lacks capacity.

5. Scope

This Policy applies to all confidential personal information staff encounter in the course of their work, however it is stored or disclosed

6. Sharing Information

The principles

The principles set out below are intended to help practitioners working with children, young people, parents and carers share information between organisations. Practitioners should use their judgement when making decisions on what information to share and when and should follow organisation procedures or consult with their manager if in doubt. **The most important consideration is whether sharing information is likely to safeguard and protect a child**.

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. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

Secure

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.

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.

7. When and how to share information

When asked to share information, you should consider the following questions to help you decide if and when to share. If the decision is taken to share, you should consider how best to effectively share the information. A flowchart follows the text.

When

Is there a clear and legitimate purpose for sharing information?
• Yes – see next question

• No – do not share

Does the information enable an individual to be identified?
• Yes – see next question

• No – you can share but should consider how

Is the information confidential?
• Yes – see next question

• No – you can share but should consider how

Do you have consent?
• Yes – you can share but should consider how

• No – see next question

Is there another reason to share information such as to fulfil a public function or to protect the vital interests of the information subject?
• Yes – you can share but should consider how

• No – do not share

How

• Identify how much information to share

• Distinguish fact from opinion

• Ensure that you are giving the right information to the right individual

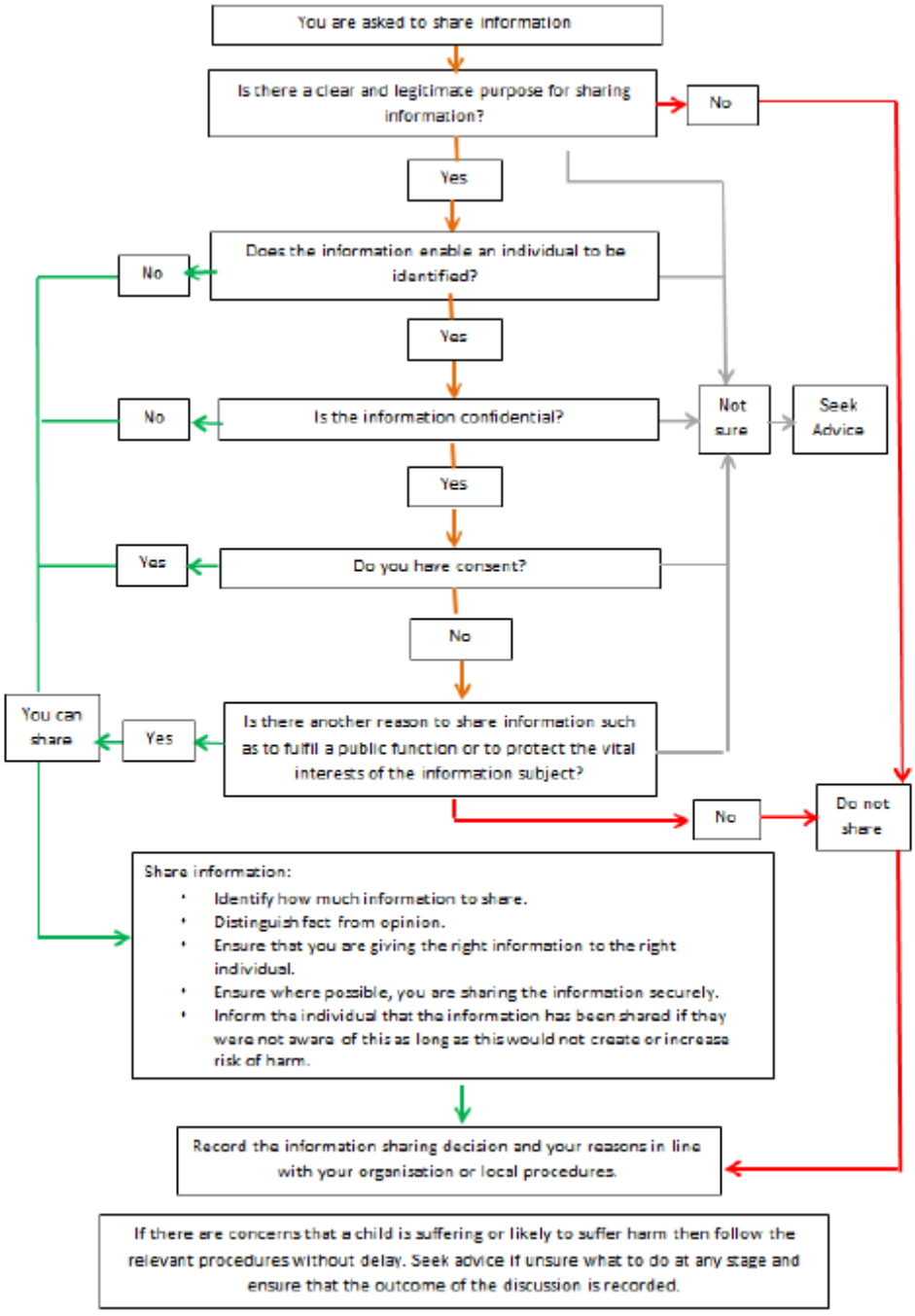
• Ensure where possible that you are sharing the information securely
Inform the individual that the information has been shared if they were not aware of this, as long as this would not create or increase risk of harm

All information sharing decisions and reasons must be recorded in line with your organisation or local procedures. If at any stage you are unsure about how or when to share information, you should seek advice and ensure that the outcome of the discussion is recorded. If there are concerns that a child is suffering or likely to suffer harm, then follow the relevant procedures without delay.

8. The Seven Golden Rules to Sharing Information

- Remember that the Data Protection Act 1998 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
- 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.
- 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.
- 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. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.
- 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
- 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, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
- 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.

9. Flowchart of When and How to Share Information



10. Confidentiality Principles

a. Confidentiality

Manchester Settlement will take care that personal information it holds is managed with respect and in line with the expectation of confidentiality. Such information will be made available only to people who need it in connection with their duties. Staff who are given access to confidential information will only use it in the course of their work for authorised purposes. Information identifying individuals will not be passed on for purposes other than the provision, review or planning of services, except where there is a legal requirement or with the knowledge and consent of the person concerned.

b. Being open

Manchester Settlement will provide clear information for people about how information we hold about them will be used.

c. **Information security and data handling**

Information will be stored and protected, whether electronic or paper copy, in line with accepted protocols of the Data Protection Act. Confidentiality may be breached if conversations are overheard or if something printed or displayed on screen is seen by someone who should not. Induction and training for staff will be used to ensure that the risks are understood. Working environments and practices will be managed to minimise these risks.

d. **Access to personal information within record systems**

Access to record systems containing personal information will be controlled to ensure that users of the systems are restricted to the information they need to do their jobs. This means limiting which records and which parts of an individual record they can use. Staff will be instructed that when they have access to personal information they must use that access only as they are specifically authorised for their own role. They must not look at information they have access to, but do not need for work allocated to them and must take reasonable steps to avoid seeing it accidentally.

e. **Sharing information**

Sharing information, including confidential information, is essential for effective service delivery, planning and review. To ensure that personal information is shared appropriately all staff will be trained on the application of the Information Sharing Principles and must follow them. These principles apply equally to sharing information internally and externally with other organisations. Staff who are uncertain with any specific situation should consult their line manager. Manchester Settlement will ensure that people understand the circumstances in which their personal information may be shared with other agencies and that they give their informed consent. We will tell people as a matter of course when their personal information is to be shared whenever this is practicable.

f. **Limitations**

Staff cannot treat information received in the course of their duties as a personal secret. Staff are responsible for their actions and failure to act and must have the wider public welfare in mind. There may be occasions when information given in confidence must be disclosed without consent to protect someone or under some other specific legal duty. A decision to do this must be made in consultation with a manager. Exceptions to the principle of informed consent to information sharing must be demonstrated to be incompatible with the need to share the information. Examples would include protection of a child, a vulnerable person, public safety or the prevention or detection of crime.

11. Staff responsibilities

Staff are personally responsible for ensuring information they have access to is not improperly disclosed. Staff may only view and amend information that is required for your role and as you are authorised to do.

Storage

Confidential information on paper must be kept in locked storage when not in use. Responsible If staff are concerned about the security of personal information in premises or systems they should raise these concerns with their line manager

Clear Desk Policy

When you leave you desk you should ensure that any personal or confidential information is not left lying around for others to see. Lock it away in a cupboard or drawer if leaving your desk for more than a few minutes. Keep confidential information on display in your working environment to a minimum and only have data relative to the current work being carried out, including documents, computer media and data on computer screens. Take care to arrange your working environment so that confidential information on your computer screen is not visible to other people who should not see it. You will need to take particular care in an environment accessible to the public or if you receive visitors. You must always lock your

computer or log off when you leave it, even for a brief period. If your computer is out of your sight then it should be locked.

Disposal of Confidential Information
Confidential information on paper must be destroyed by shredding. Removable media such as floppy disks or CDs containing confidential information should be physically destroyed when no longer needed. Reusable electronic media (such as USB flash drives) should have their contents securely deleted.

Sharing information with third parties
See Guidance in this policy

Telephones
If a request for information is made by telephone, always try to check the identity of the caller **and** check whether they are entitled to the information they request and take a number, verify it independently and call back if necessary.

Take care that you do not have sensitive conversations where they can be overheard. It is very easy to become unaware of your surroundings when talking on a mobile phone. Think before you start the phone call.

Take care when you leave messages on an answering machine or voicemail, or if sending a text message. You do not know who will pick them up. If the person you want to reach would be embarrassed if someone else knew you were calling them take that into account.

Mobile phones may retain personal information such as records of calls made and text messages you have sent. Delete personal information from the phone as soon as possible. Lock the phone when not using it

Use of Internal and External Post
It is all too easy to make mistakes with the post, especially when a lot of similar items are being sent out at once. Check to make sure that the envelope is addressed correctly and that the right information is going in it.

Fax
If you are sending a fax containing personally-identifiable information double check the fax number before sending. Make sure someone is waiting at the other end.

Staff should be aware of updates to guidance available from the DfE such as

12. Contractual Obligations

The staff contract makes specific reference to confidentiality obligations that apply during and after an employment period.

13. Resources

https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice