Hillingdon LSCB Multi-agency Information Sharing Protocol

July 2016

Contents

1. Introduction 3
2. Scope 3
3. Limits of this Information Sharing Guidance 3
4. The legal context 4
5. Information sharing and child protection 4
6. Issues of confidentiality 5
7. Consent 5
8. Children / Young People & Consent 6
9. Parental Responsibility & Consent 6
10. Sharing information without consent 7
11. Key considerations 8
12. Information Retention and Disposal 10
13. Caldicott principles 11

Appendix 1 12

Appendix 2 13

Appendix 3 14

Appendix 4 14

1. Introduction

Working Together to Safeguard Children 2015 identified that "Effective sharing of information between professionals and local agencies is essential for effective identification, assessment and service provision. Early sharing of information is the key to providing effective early help where there are emerging problems."

And yet the Department of Education's triennial analysis of Serious Case Reviews illustrates that there is evidence of uncertainty amongst practitioners about how and when to share information, despite national guidance."

This guidance therefore has been written to support a culture of information sharing in Hillingdon, underpinned by all professionals being informed of the guidance within this area.

2. Scope

This document does not replace any individual information sharing agreements between partner agencies and this document should be read in conjunction with your own agency's policies and procedures governing information sharing to safeguard children. Where any conflict between local procedures and this protocol is identified this should be discussed with a senior manager within the agency concerned, it should also be reported to Hillingdon Local Children Safeguarding Board.

This guidance draws upon the guidance issued by the Department for Education and London Multi-agency safeguarding procedures. Consideration has also been given to the findings of the Munroe report, and various serious case reviews. A full list of references is available in Appendix 4.

3. Limits of this Information Sharing Guidance

This Protocol does not apply to actions taken within the Multi-Agency Safeguarding Hub (MASH). The MASH has its own Information Sharing Protocol covering its internal business.

This protocol does not apply to intelligence sharing between Children's social care and The Metropolitan Police, where a separate Guidance for Sharing CSE Information with Police is available, alongside information sharing form.

This protocol does not apply in respect of patient or service-user access to records or Disclosure of information in cases of alleged child abuse and linked criminal and care directions hearings.

4. The legal context

The key legislation 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

5. Information sharing and child protection

Fears about sharing information cannot be allowed to stand in the way of the need to promote the welfare and protect the safety of children. Whilst the Data Protection Act 1998 places duties on organisations and individuals to process personal information *fairly and lawfully*, it is not a barrier to sharing information where the failure to do so would result in a child or vulnerable adult being placed at risk of harm. Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns.

If you have concerns about a child's welfare, or believe they are at risk of harm, you should share the information with Hillingdon Children's Services via Hillingdon MASH.

There are no insurmountable legal barriers to sharing information appropriately, and a demonstrably proportionate sharing of information can be justified as being in the public interest.

If you think a crime has been committed and/or a child is at immediate risk, you should notify the police without delay.

6. Issues of confidentiality

Confidential information is defined as:

- Personal information of a private or sensitive nature; and
- Information that is not already lawfully in the public domain or readily available from another public source; and
- Information that has been shared in circumstances where the person giving information could reasonably expect that it would not be shared with others.

People may not specifically ask you to keep information confidential when they discuss their own issues or pass on information about others, but may assume that personal information will be treated as confidential. In these situations you should check with the individual whether the information is or is not confidential, the limits around confidentiality and under what circumstances information may or may not be shared with others.

The key principles of sharing information can be found in the seven golden rules to sharing information, laid out in appendix 2.

Remember: No review into multi- agency working has ever criticised practitioners for sharing too much information regarding child protection concerns.

7. Consent

Obtaining explicit consent for information sharing is best practice and ideally should be obtained at the start of the involvement, when working with the individual or family to agree what support is required. It can be expressed either verbally or in writing. Written consent is preferable as it provides evidence that consent was given and therefore reduces the scope for subsequent dispute.

Consent must be 'informed' - this means that the person giving consent needs to understand why information needs to be shared, what will be shared, who will see their information, the purpose to which it will be put and the implications of sharing that information.

Being declined consent to share information does not prevent a referral being made to Hillingdon MASH where you have child protection concerns.

8. Children / Young People & Consent

A young person aged 16 & 17 are presumed in law to have capacity to make their own decisions, including consent to information sharing.

Children aged 12 or over may generally be expected to have sufficient understanding and some younger children may also have sufficient understanding.

When assessing whether a particular child on a particular occasion has sufficient understanding to consent, or refuse consent, to sharing of information about them, consider:

- Can the child understand the question being asked of them?
- Does the child have a reasonable understanding of:
    - What information might be shared?
    - The main reason or reasons for sharing the information?
    - The implications of sharing that information, and of not sharing it?
- Can the child:
    - Appreciate and consider the alternative courses of action open to them?
    - Weigh up one aspect of the situation against another?
    - Express a clear personal view on the matter, as distinct from repeating what someone else thinks they should do?
    - Be reasonably consistent in their view on the matter, or are they constantly changing their mind?

If the child / young person does chose to share information with you, be sure to act on it.

9. Parental Responsibility & Consent

In most cases, where a child cannot consent or where you have judged that they are not competent to consent, a person with Parental Responsibility should be asked to consent on behalf of the child.

If a child is judged not to have the capacity to make decisions, their views should still be sought as far as possible.

Where parental consent is required, the consent of one such person is sufficient. In situations where family members are in conflict you will need to consider carefully whose consent should be sought. If the parents are separated, the consent of the parent with *whom the child resides* would usually be sought.

If the child is subject to a Care Order, practitioners should liaise with the relevant local authority about questions of consent.

You should try to work with all involved to reach an agreement or understanding of the information to be shared. You must always act in accordance with your professional code of practice where there is one and consider the safety and wellbeing of the child, even where that means overriding refusal to consent.

If you are unsure seek advice from your manager or designated safeguarding adviser

10. Sharing information without consent

You do not necessarily need the consent of the information subject to share their personal information. Wherever possible, you should seek consent or be open and honest with the individual (and/or their family, where appropriate) from the outset as to why, what, how and with whom, their information will be shared.

When there is evidence or reasonable cause to believe that a child is suffering, or is at risk of suffering, significant harm, or information relates to the prevention of significant harm to a child or serious harm to an adult (including through the prevention, detection and prosecution of serious crime), then sharing confidential information without consent will almost certainly be justified on the basis that it is in the public interest.

When you should NOT seek consent

There will be circumstances where you should **not seek** consent from the individual or their family, or inform them that the information will be shared, for example where to do so would:

- Place a child at increased risk of Significant Harm
- Place an adult at risk of serious harm
- Prejudice the prevention, detection or prosecution of a serious crime (i.e. a crime involving Significant Harm to a child or serious harm to an adult)
- Lead to unjustified delay in making enquiries about allegations of Significant Harm to a child or serious harm to an adult.

11. Key considerations

The law says that information should be adequate, relevant, not excessive, accurate and up to date and therefore some key considerations in sharing information:

- You should check the quality of information before it is shared to minimise the spreading of inaccuracies across information systems.
- Be alert to variations in data recording practice. For example, a person's date of birth, or even name, can be recorded in various formats. This can lead to records being mismatched, duplicated or corrupted. Before sharing information you must make sure that the organisations and partners involved have a common way of recording key information.
- Having a clearly defined objective will help you to determine what information is necessary to achieve that objective. You must never share information if it is **not necessary** to do so.
- If you have any doubt, seek advice from your manager or designated safeguarding lead.
- Avoid the use of jargon, acronyms or information which is ambiguous
- You should record all information sharing decisions and the reasons for it whether or not you decide to share information. If the decision is to share, you should record what information was shared, with whom and in what format.

Information shared should be necessary for the purpose and proportionate.

Methods Used for sharing information

Access to personal information should be on a strict need-to-know basis. Only staff that need access to personal identifiable information should have access to it, and they should only have access to the information items that they need to see.

Remember:
Personal files must never be left unattended or unsupervised. This means that, outside normal working hours, they must be locked away in cabinet

Codes for accessing computers must never be noted in such a way that others can see and use them.

The conveying of information needs to be achieved in a secure way.

Information may be transferred in the following ways:

- Verbally, face to face, in meetings or on the telephone.
- In written communications, (for example, forms, minutes, letters, statements or reports)
- Transferred in hard copy through internal or external mail services.
- Documents transferred on encrypted electronic digital media devices.
- In written information transferred by secure email, or secure file transfer systems.
- Information accessed in situ, via provision of access to organisational databases or records.

When each of these methods is used it is essential to consider the safest way to record and mark the information, and to ensure safe transit and delivery. Information should be appropriately secured in transit, transferred by methods aligned to the best practice specified in the "Protecting Information in Government Report – January 2010".

a) Verbal conversations and interviews should be recorded in a written statement. Care must be taken to record and denote information clearly as fact, statement or opinion and to attribute any statement or opinion to the owner. All information should be recorded in such a way that it can be used as evidence in court, should that be required at a later date.

b) Meetings should be recorded in minutes that are agreed by all attendees.

c) Written communications containing confidential information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation. They should be clearly marked "Private & Confidential – to be opened by the recipient only".

d) When files are transferred on electronic digital media devices, the files should be encrypted to an appropriate standard, with decryption keys / passwords supplied separately.

e) When confidential information is sent by email, it should be sent and received using secure government domain email addresses, to ensure encryption of information in transit. The full list of secure Government email systems are found is below.

    - .cjsm.net (Criminal and Justice)
    - .gcsx.gov.uk (Local Government/Social Services)
    - .gse.gov.uk (Central Government)

- .gsi.gov.uk (Central Government including Department of Health)
- .gsx.gov.uk (Central Government)
- .hscic.gov.uk (The Health and Social Care Information Centre)
- .mod.uk (Military)
- .nhs.net (NHSmail)
- .pnn.police.uk (Police)
- .scn.gov.uk (Criminal and Justice)

Security of these systems is reliant on BOTH the sender AND recipient using one of the email domains listed above.

In all transfer scenarios, the onus is on the SENDER to ensure that:

- Information is transferred securely
- The chosen method is acceptable to and workable by the recipient
- Information has reached the required recipient

In the event that a recipient receives information by an unsecured route, it is the responsibility of the recipient to advise the sender and agree a secure route for future transfers of information. This can include the use of Egress Switch encryption.

12. Information Retention and Disposal

The Data Protection Act (1998) requires that personal data and sensitive personal data is not retained for longer than necessary. Partner organisations may have their own organisational, legal or procedural requirements for records retention and disposal. These retention schedules should be observed and applied at all times.

Where no such organisational procedure exists, you will need to use your professional judgement and give consideration to:

- The current and future value of the information for the purpose for which it is held
- Costs, risks and liabilities associated with retaining the information
- The ease or difficulty of making sure the information remains accurate and up to date

13. Caldicott principles

Caldicott principles relate to all health and social care organisations and each organisation will have internal guidance. It is important that all professionals ensure they are aware of the guidance and know who their Caldicott Guardian is. The Calidcott principles are listed in appendix 2.

All agencies should ensure that staff have access to training and refresher training on information sharing to ensure that all the workforce is confident in how they share information.

Appendix 1

Hillingdon Local Safeguarding Children Board members

- Border Force (part of the Home Office)
- CAFCASS
- Central and North West London NHS Foundation Trust.
- Healthwatch Hillingdon
- Hillingdon Clinical Commissioning Group
- Hillingdon Inter Faith Network
- Home Office
- London Ambulance Service NHS Trust
- London Borough of Hillingdon
- London Community Rehabilitation Company
- London Fire Brigade
- London Probation
- Metropolitan Police Service
- SSAFA
- The Hillingdon Hospitals NHS Foundation Trust

Appendix 2

The seven golden rules to sharing information

1. 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.

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. 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.

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, 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).

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.

Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers - March 2015

Appendix 3

Caldicott Principle

Principle 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.

Principle 2
Don't use patient-identifiable information unless it is absolutely necessary
Patient-identifiable data items should not be used unless there is no alternative.

Principle 3
Use the minimum necessary patient-identifiable information
Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

Principle 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.

Principle 5
Everyone 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.

Principle 6
Understand and comply with the law
Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

Principle 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.

Appendix 4

Additional guidance

Here are resources for all practitioners who come into contact with children, young people and their families in London Borough of Hillingdon:

Working Together to Safeguard children (2015)

Keeping Children Safe in Education (2015)

What to do if you're worried a child is being abused (2015)

Pathways to harm, pathways to protection: a triennial analysis of serious case reviews 2011 to 2014: Final report (2016)
Department of Health.

ICO Data Sharing Code of Practice for Sharing of Personal Data
Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

Information Sharing: Guidance for Practitioners and Managers [1] (HM Government, March 2009)
Available at: http://webarchive.nationalarchives.gov.uk/20100623194820/publications.everychildmatters.gov.uk/eorderingdownload/00807-2008bkt-en-march09.pdf

London Child Protection Procedures and Practice Guidance

Available at http://www.londoncp.co.uk/

Information Sharing: Pocket guide (HM Government, 2008)

How to identify which rules apply when sharing information (DfE, 2011)

How to record decisions (DfE, 2011)

How to seek consent (DfE, 2011)

How to share information securely (DfE, 2011)

How to judge capacity to give consent (DfE, 2011)