LSCB Information Sharing Protocol

Date of next review	June 2018
Date of last review	June 2017
Date of approval	May 2015

CONTENTS

Information Sharing

Sharing information is an intrinsic part of any frontline professionals 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 service at the right time and prevent 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 in serious case reviews carried out following the death of, or serious injury to a child.

Fear about information sharing 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. Those skilled practitioners are in the best position to use their professional judgement about when to share information with colleagues working in the same organisation as well as with those working in other organisations, in order to provide effective early help and to keep children safe from harm.

Being alert to the signs of abuse and neglect and taking action

All practitioners should be alert to the signs and triggers of child abuse and neglect (see appendix Early Help safeguarding Strategy and threshold document) Abuse (emotional, physical, sexual) and neglect can present in many different forms. Indicators of abuse and neglect may be difficult to spot. Children may disclose abuse, in which case the decision to share information is clear. In other cases the indicators may be more subtle and appear over time. In these cases decisions about what information to share and when, will be more difficult to judge. Everyone should be aware of the potential for children to be sexually exploited for money, power or status and individuals should adopt an open and inquiring mind to what could be underlying reasons for behaviour changes in children of all ages. If a practitioner has concerns about a child's welfare, or believes they are at risk of harm, they should share information with children's social care or the police. Security of information should be considered and should be proportionate to the sensitivity of the information and the circumstances. If it is thought a crime has been committed and or a child is at immediate risk the police should be notified without delay.

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 put a child or vulnerable adult being placed at risk of harm. Similarly human rights concerns, such as respecting the right to a private family life would not prevent sharing where there are real safeguarding concerns.

The LSCB has a strong role in supporting information sharing between and within organisations and addressing barriers to information sharing.

The LSCB can require an individual or body to comply with a request for information as outlined in section 14B of the Children Act 2004.

To ensure effective safeguarding arrangements:

- all organisations should have arrangements in place which sets out clearly the processes and the principles for sharing information between each other, with other professionals and with the LSCB; and
- no professional should assume that someone else will pass on information which they think will be critical to keeping a child safe. If a professional has concerns about a child's welfare and believes they are suffering or likely to suffer harm, then they should share the information with local authority children's social care.

Information sharing: advice for practitioners providing safeguarding services to children, young people, parents and carers (2015) supports front line practitioners, working in child or adult services, who have to make decisions about sharing personal information on a case by case basis.

Seven golden rules for information sharing

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.

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 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 a appropriate, secure way. Practitioners must always follow their organisations 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 with whom, in line with 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 iwht the organisations 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.

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.

Information Sharing Checklist

Question 1:	Is there a clear and legitimate purpose of sharing information?	
Question 2:	Does the information enable a living person to be identified?	
Question 3:	Is the information confidential?	
Question 4:	Do you have consent to share?	
Question 5:	Is there sufficient public interest to share information?	
Question 6:	Are you sharing information appropriately and securely?	
Question 7:	Have you properly recorded your information sharing decision?	

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 it would not create increase risk of harm.**

Application

This protocol applies to all LSCB agencies in North Lincolnshire and service providers commissioned by LSCB agencies. Voluntary agencies and other bodies involved in LSCB procedures are encouraged to use the protocol for guidance.

The Purpose(s) of this information sharing protocol

The purpose of sharing information within the Community is to:

- Ensure the provision of appropriate services for children 'in need', or at risk or likely to be at risk of suffering significant harm (Sections 17 (10) and 47 (1) of the Children Act 1989) or who otherwise are considered to be at risk of social or educational exclusion.
- By sharing information, the Community will be able to identify children considered to be 'in need' or at risk of social or educational exclusion at an early stage of concern and provide effective multi-agency intervention in order to promote their health and well-being.
- Personal information should not be shared if it does not meet one of these purposes.

Information provided for one purpose should not be used for another purpose without consideration being given as to whether further consent is needed. However, where

information is being shared to prevent or reduce crime, or in connection with the safety and well-being of a child, further consent will not normally be necessary.

Relevant legislation:

- Children Act 1989 (Sections 17, 27 and 47)
- Local Government Act 2000 (Section 2)
- Crime and Disorder Act 1998 (Section 115)
- Data Protection Act 1998 (Part IV).
- Learning & Skills Act 2000
- Children Act 2004 (Section 11) Obtain assistance for the local authority from other agencies in order for the local authority to perform its functions of providing services to children and families under Part III, Section 27, of the Children Act 1989.
- Promote or improve the economic, social or environmental well-being of children and families in need within North Lincolnshire. This will include provision of improvements to health and/or educational opportunity as well as the reduction or elimination of risk factors for children within the area. (Section 2, Local Government Act 2000, Learning & Skills Act 2000).
- Prevent or reduce crime and identify and apprehend offenders or suspected offenders (Section 115, Crime and Disorder Act 1998).
- Co-operate to safeguard children, improve well-being and promote their welfare (statutory guidance under Section 11 of the Children Act 2004)
- Information sharing: Guidance for practitioners and managers DCSF 2008
- Section 14 A of the Children Act 2004 which was inserted by section 8 of the Children, Schools and Families Act 2010.

Information/Data to be shared – Key Principles

The Community will share information (for the purposes of this protocol, information and data are taken to be the same thing) in accordance with the requirements of the Data Protection Act 1998 and in-line with guidance issued by the government on information sharing in October 2015.

Information will also be shared in accordance with Caldicott Principles

- Justify the purpose(s)
- Don't use personal confidential data unless it is absolutely necessary
- Use the minimum necessary personal confidential data
- Access to personal confidential data should be on a strict need –to-know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Comply with the law and
- The duty to share information can be as important as the as the duty to protect patient confidentiality

Consent will normally be required where information is to be shared that allows the identification of an individual. Consent is not required if a) data is "de-personalised", making it impossible to identify an individual from the shared information, or b) if the information is subject to any of the exemptions under the Data Protection Act 1998.

Agencies and professionals should also follow the Seven Golden Rules for Information Sharing DfE 2015, cited above.

Remember that the Data Protection Act is not a barrier to sharing information

The *' Seven Golden Rules'* and the Questions above will help support your decision making so you can be more confident that information is being shared legally and professionally. If you answer *'not sure'* to any of the questions, seek advice from your supervisor, manager, nominated person within your organisation or area, or from a professional body.

The sharing of healthcare related information or data will continue to be governed by relevant guidance, including but not limited to:

- NHS Care Record Guarantee
- NHS Confidentiality Code of Practice
- Caldicott Guidance

Agencies will work together, and without delay, in the sharing of information critical to safety and care of individuals. All parties are reminded of their individual obligation to protect the confidential nature of the information they may hold. It is understood that, at times, this may prevent the automatic sharing of data.

De personalised information

The Data Protection Act places no restrictions on the disclosure of data which does not identify individuals. If de-personalised data can be used for information sharing purposes there will be no data protection implications. However, parties should take care that data that has been "de-personalised" could not become attributable to an individual using information that may be already held or obtained by other means (e.g. unique identifier obtained from another list).

Personal Information

Any disclosure of personal information must have regard to both common and statute law, for example defamation, the common law duty of confidence and the Data Protection principles.

The Data Protection principles require that:

- Personal data shall be processed fairly and lawfully.
- 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.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Security measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles must be adhered to by all participants of this information sharing protocol.

The extent of any personal information disclosed will be limited to that which is relevant to the purpose or purposes for which the information was requested and shared only with appropriate agencies.

Personal data will not be kept for longer than is necessary for the purpose for which it was provided; after which it will be destroyed by the parties to this Protocol, other than the data originator who will review the data in accordance with agreed policy.

Consent

Prior to sharing information the issue of consent must be considered. If clear, explicit and informed consent is provided in writing for the processing of the data then the processing should be possible without concern.

Consent should be obtained from all those persons who are identifiable from the information; this will include client, patient, victim, perpetrator, informant etc.

Consent should be included within a consent form signed by the data subject. It is possible to share information without consent but this should only be considered if the obtaining of consent is inappropriate given the facts of any particular case. This would include where there is a Police investigation, where consent seeking would put a person in danger etc.

Each agency should provide guidelines to their workers to ensure that they are complying fully with the Act when receiving or disclosing information without consent of the subject of the data.

It is important to note that you do not necessarily need the consent of the information subject to share personal information. Wherever possible you should seek consent or be open and honest with the individual (and or the family where appropriate) from the outset as to what, what, how and with whom their information will be shared. You should seek consent where an individual may not expect their information to be passed on and they have a genuine choice about this Consent in relation to personal information does not need to be explicit – it can be implied where to do so would be reasonable. Even without consent it is still possible to share personal information if t is necessary in order to carry out your role, or to protect the vital interests of the individual where for example, consent cannot be given.

Also if it is unsafe or inappropriate to do so, ie where there are concerns that a child is suffering, or is likely to suffer significant harm, you would not need to seek consent. A record should be kept of what has been shared.

Consent is withheld

Where a person provides information but wishes for the information to be kept in confidence, that confidentiality should be respected. If however there is an overriding interest in the disclosing of such information, it can be disclosed. Such overriding interests would include where the information is required to be disclosed to prevent significant harm to a child, for the prevention/detection of crime etc. Where information is confidential, disclosure should be limited as far as possible to those persons or agencies that need to know and should be the minimum information necessary to meet the need for disclosure.

Disclosures

When disclosing personal information, many of the data protection issues surrounding disclosure can be avoided if the consent of the individual concerned has been sought and obtained.

A recipient of personal information must obtain the consent of the data originator before making a secondary disclosure to another party to this Protocol or where there is a pressing need to disclose information, as set out in the Information Sharing Code of Practice 2006, page 8, Section 8. For the purpose of this requirement, each local authority department will be treated as a separate agency. Children's Services will be treated as a single agency.

The Extent of Disclosure

Agencies may hold a lot of data about a particular person, however consideration should be given as to the extent of the disclosure to be made. Disclosure should not be made of information that is not relevant. Each agency will need to consider what information they hold and what is necessary to be disclosed for that purpose.

Security

Each agency must ensure that any data it maintains about an individual is securely stored. Access to such information must be limited to those who need to know and should be proportionate to the nature of the information i.e. the more sensitive the data the more securely it is stored. Agencies are asked to respect requests for confidentiality of data that is disclosed under the LSCB procedure.

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. We will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal information whether intentional or inadvertent.

Sub Judice

Where the Police are in the process of investigating a criminal offence, disclosure of information is restricted so as to not prejudice any trial/investigation. Where evidence gathered for the purpose of a trial is required for the purposes of LSCB procedures to protect a child, the Police will liaise with the CPS as to what evidence may or should be disclosed.

Subject Access

Under Data Protection legislation, individuals have a right of access to any information held about themselves. This right may be denied in certain limited circumstances, which include where access would prejudice the prevention and detection of crime.

A person does not have the right to know what is recorded about someone else (a "third party") unless the consent of the third party is gained. This includes information held on family members within an individual's records.

However, the agency can decide that there may be circumstances in which it is reasonable to disclose such information without consent. In reaching this decision, the agency must have regard to:

(i) any duty of confidentiality owed to the third party;

(ii) any steps taken with a view to seeking consent of the third party to the disclosure;

(iii) whether the third party is capable of giving consent;

(iv) any express refusal of consent by the third party. *(s7(6) Data Protection Act 1998)*

Complaints

Complaints about the disclosure of information under this Protocol, or breaches of the Protocol should be dealt with under established procedures relevant to each agency.

Agreement

Where a disclosing agency provides information to a requesting agency which is inaccurate, and the requesting agency incurs liability, cost or expense as a result of its reliance upon 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;
- Where a party to this Protocol receives a request for information about an individual, and personal information which it holds is identified as belonging to another agency, it will be the responsibility of the receiving agency, through the designated officer, to contact the agency that owns the data to determine whether the latter wishes to claim an exemption under the provisions of the Data Protection Act.
- 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.

Myth busting about information sharing

The data protection Act 199 is a barrier to sharing information No- the Data protection Act 1998 does not prohibit the collections and sharing of personal information. It does, however provide a framework to ensure that personal information about a living individual is shared appropriately. In particular the Act balances the rights of the information subject (the individual whom the information is about) and the need to share information about them. Never assume sharing is prohibited- it is essential to consider this balance in every case.

For further information see the Information Commissioner statutory code of practice

Personal information collected by one organisation cannot be disclosed to another organisation.

This is not the case, unless the information is to be used for a purpose incompatible with the purpose that it was originally collected for. In the case of a child at risk of significant harm, it is difficult to foresee circumstances where sharing personal information with other practitioners would be incompatible with the purpose for which it was originally collected.

The common law duty of confidence and the Human Rights Act 1998 prevent the sharing of personal information. No- this is not the case. In addition to considering to considering the Data protection Act 1998 local responders need to balance the common law duty of confidence and the rights within the Human Rights Act 1998 against the effect on individuals or others of not sharing the information.

If information collection and sharing is to take place with the consent (implied or explicit) of the individuals involved, providing they are clearly informed about the purpose of the sharing, there should be no breach of confidentiality or breach of the human Rights Act 1998. If the information is confidential and the consent of the information subject is not gained, then the responder needs to satisfy themselves that there are grounds to override the duty of confidentiality in these circumstances. This can be because it is overwhelmingly in the information subjects interests for this information to be disclosed. It is possible that an overriding public interest would justify disclosure of the information.

To overcome the common law duty of confidence, the public interest threshold is not necessarily difficult to meet- particularly in emergency situations. Confidential health information carries a higher threshold, but it should still be possible to proceed where the circumstances are serious enough.

IT systems are often a barrier to effective information sharing

Professional judgement is the most essential aspect of multi-agency work, which could be put at risk if organisations rely too heavily on IT systems. There are also issues around compatibility across organisations along with practitioners who may have the knowledge and understanding of how to use them.

Flowchart of when and how to share information