Information Sharing Agreement (ISA) for the purposes of Safeguarding Children

This Information Sharing Agreement (ISA) sits beneath the overarching Information Sharing Protocol (ISP)/Partnership Agreement to which the Partners listed below are signatories.

There are other reasons for agencies to share information which are not covered by this agreement, such as the obligation for agencies to share information with their regulators for the purpose of assurance.

The appendices provide further information and guidance for staff including the Government Guidance, Every Child Matters and the "Information sharing advice for safeguarding practitioners 2015".

See Appendix A for further detail regarding this.

1. Partners/signatories

Partners	Addresses
Local Authorities	
Leicestershire County Council	County Hall, Glenfield, Leicester, LE3 8RA
Leicester City Council	91 Granby St, Leicester, LE1 6FB
Rutland County Council	Catmose, Park Rd, Oakham, Rutland, LE15 6HP
Leicester City Youth Offending Service	Eagle House, 11 Friar Lane, Leicester, LE1 5RB
Leicestershire Youth Offending Service	County Hall, Glenfield, Leicester, LE3 8RA
Police	
Leicestershire Police	Force Headquarters, St Johns, Enderby, Leicester, LE19 2BX
Probation Agencies/Organisations	
National Probation Service Midland Region	National Probation Service, 1 Victoria Square, Birmingham, B1 1BD

Derbyshire, Leicestershire, Lincolnshire, Nottinghamshire & Rutland Community Rehabilitation Company LTD	2 St John Street, Leicester, LE1 3WL
Fire & Rescue	
Leicestershire Fire & Rescue Service	12 Geoff Monk Way, Birstall, Leicester, LE4 3BU
Health Agencies/Organisations	
NHS England (Leicestershire & Lincolnshire Team)	Fosse House, 6 Smith Way, Grove Park, Enderby, Leicestershire, LE19 1SX
East Leicestershire and Rutland Clinical Commissioning Group	Unit 2-3 (Ground Floor), Bridge Business Park, 674 Melton Road, Thurmaston, Leicestershire, LE4 8BL
West Leicestershire Clinical Commissioning Group	55 Woodgate, Loughborough, Leicestershire, LE11 2TZ
Leicester City Clinical Commissioning Group	St John's House, 30 East Street, Leicester, LE1 6NB
University Hospitals of Leicester NHS Trust	Level 3, Balmoral Building, Leicester Royal Infirmary, Infirmary Square, Leicester, LE1 5WW
Leicestershire Partnership NHS Trust	Riverside House, Bridge Park Plaza, Bridge Park Road, Thurmaston, Leicester, LE4 8PQ
East Midlands Ambulance Service NHS Trust	1 Horizon Place, Mellors Way, Nottingham Business Park, Nottingham, NG8 6PY
District Councils	
Blaby District Council	Council Offices, Desford Road, Narborough, Leicestershire, LE19 2EP
Charnwood Borough Council	Southfield Rd, Loughborough, Leicestershire, LE11 2TN
Harborough District Council	The Symington Building, Adam and Eve St, Market Harborough, Leicestershire, LE16 7AG
Hinckley and Bosworth Borough Council	Hinckley Hub, Rugby Road, Hinckley, Leicestershire, LE10 0FR

Melton Borough Council	Parkside, Burton Street, Station Approach, Melton Mowbray, Leicestershire, LE13 1GH
North West Leicestershire District Council	Council Offices, Whitwick Road, Coalville, Leicestershire, LE67 3FJ
Oadby and Wigston Borough Council	Station Rd, Oadby, Wigston, Leicestershire, LE18 2DR
Other Agencies/Organisations	
CAFCASS	49 Western Blvd, Leicester, LE2 7HN
Barnardo's	West Point, Feldspar Close, Enderby, Leicestershire, LE19 4SD
New Futures Project	Sussex St, Leicester, LE5 3BF
Voluntary Action Leicestershire	9, Newarke St, Leicester, LE1 5SN
NSPCC	NSPCC Midlands, 3rd Floor CIBA Building, 146 Hagley Road, Birmingham, B16 9NP
Glebe House (Signed 4.10.2016)	Woodgate Chambers, 70, Woodgate Loughborough, Leicestershire LE11 2 TZ
Diocese of Leicester (Signed 21.12.16)	St Martins House 7, Peacock Lane Leicester LE1 5PZ

2. Purpose – Why do you need to share this information?

The purpose of this Information Sharing Agreement is to facilitate the lawful sharing of information in order to safeguard children and young people: when sharing information in response to managing child protection concerns, and when these are encountered amongst the children, young people and families they are working with. It should be read in conjunction with the Leicester, Leicestershire & Rutland Safeguarding Children Procedures.

3. Legal Basis – What law allows you to share this information?

Information must be shared lawfully. If you are a public authority you can only work within legal framework which relates to your agency/organisation (Ultra vires rule).

Section 10 of the Children Act 2004 places a duty on each local authority in England to make arrangements to promote cooperation between:

(a) The authority

(b) Each of the authority's relevant partners

and

(c) Such other persons or bodies as the authority consider appropriate, being persons or bodies of any nature who exercise functions or are engaged in activities in relation to children in the authority's area.

Child Protection

Section 47(1) of the Children Act 1989 states that:

Where a local authority:

(a) is informed that a child who lives, or is found, in their area (i) is the subject of an emergency protection order, or (ii) is in police protection

and

(b) have reasonable cause to suspect that a child who lives, or is found, in their area is suffering, or is likely to suffer, significant harm:

the authority shall make, or cause to be made, such enquires as they consider necessary to enable them to decide whether they should take any action to safeguard and promote the child's welfare.

For more information see Appendix B.

Children in need

Section 17(10) states that a child shall be taken to be in need if:

(a) The child is unlikely to achieve or maintain, or to have the opportunity of achieving or maintaining, a reasonable standard of health or development without the provision of services by a local authority under Part III of the Children Act 1989

(b) The child's health or development is likely to be significantly impaired, or further impaired, without the provision of such services

(c) The child is disabled.

Early Help and prevention

Early Help and prevention is about how different agencies work together to help children, young people and their families, at any point in their lives, to prevent or reduce difficulties.

Although Early Help does not provide a lawful basis for sharing information, the requirements to be met under the Data Protection Act 1998 can be fulfilled by obtaining explicit consent in writing from the person whose personal data you intend to share.

More information about Early Help and thresholds to other services for children and families across Leicester, Leicestershire and Rutland can be found using the following link – http://lrsb.org.uk/local-guidance

For more information see Appendix B to this document.

Data Protection Act 1998 (DPA)

The DPA does not give a legal basis to share information; however the requirements of the DPA must be satisfied.

Personal data is information which relates to any individual who can be identified from the data or from the data and other information held by the data controller as defined in section 1 of the DPA.

Sensitive personal data means personal data consisting of information relating to:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Whether the individual is a member of a trade union
- Their physical or mental health or condition
- Their sexual life
- The commission or alleged commission by them of any offence
- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The DPA sets out additional safeguards for any processing of sensitive personal data.

Where there is a need to share personal and sensitive personal data each partner must be able to identify a condition in schedule 2. If sensitive personal data is being shared, a schedule 3 condition must also be identified before the information can be processed and shared.

Human Rights Act 1998 (HRA)

The HRA applies to all public authorities, and parties to this agreement endeavour to ensure that principles of the HRA are enshrined in their actions. Proportionality has been identified as the key to Human Rights compliance. This means striking a fair balance between the rights of the individual and those of the rest of the community. There must be a reasonable relationship between the aim to be achieved and the means used.

Article 8 of the Human Rights Act 1998 states that everyone has the right to respect for his private and family life, his home and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law. As personal and sensitive personal data is to be shared to implement this Information Sharing Agreement, it has been identified as necessary to enable

effective identification of, and appropriate support and intervention for, children and young persons who require safeguarding in order to prevent crime, to protect health and to protect their rights and freedoms. This sharing justifies interference with an individual's Article 8 rights.

The partners will share the minimum amount of personal data and sensitive personal data necessary to achieve the purpose identified above. This is to ensure the information shared is proportionate to the purpose and justifies the interference with the Article 8 rights of the data subjects.

You need to remember that some information is protected from sharing or disclosure by legislation or Home Office guidance (certain health information, convictions) so you need to make sure that no such restrictions apply to the information you want to share.

4. Information sharing with Consent

Many issues surrounding the disclosure of personal information can be avoided if informed consent of the individual has been sought and obtained. Obtaining consent, in circumstances where it is appropriate and possible, remains a matter of good practice. Practitioners should encourage patients and clients to see information sharing in a positive way, as something which supports the provision of effective services.

5. Information sharing without consent

Practitioners should not seek consent when they are required by law to share information through a statutory duty or by a court order. Consent should also not be sought if doing so would:

- Place a person (individual, family member, staff or a third party) at increased risk of significant harm
- Prejudice the prevention, detection or prosecution of a serious crime
- Lead to an unjustified delay in making enquiries about allegations of significant harm to an adult.

If consent has not been sought, or sought and withheld, the agency must consider if there is a legitimate purpose for sharing the information and if it is in the public interest to share.

6. Information sharing with charities

There are a number of charitable organisations that offer support to children and young people. Such organisations are not created under statute and therefore do not have statutory powers; nevertheless, they are often able to offer help and assistance in the form of counselling, advice, support and guidance as well as referring individuals to other organisations and charities within their network.

Before any information sharing is undertaken, consent should be sought from the individual wherever possible as previously stated in section 4. However, there may be circumstances where, even though consent has not been given, it is evident, taking into account the risk assessment and all of the information around the case,

that a charitable organisation can provide the support required to help safeguard children. In such cases where a decision is made to share an individual's information without their consent, a record should be kept to record the justification for making the referral without consent.

The minimum amount of information should be disclosed to achieve the objective. For example, when referring a child victim of abuse it may not be appropriate to disclose their injuries sustained, but it may be appropriate for the safety of agencies involved to disclose the details of the perpetrator. When referring a perpetrator, then the details of the victim may need to be disclosed. It may be necessary to provide relevant information regarding the risk assessment. For example, safe means and times of contact. (Disclosure must be considered on a case by case basis and proportionate to the situation.)

7. People lacking capacity

When sharing information in respect of adults who lack the capacity to provide any required consent, information should only be shared when it is permitted by relevant legislation and if considered to be in the person's best interests.

Additionally, where a person lacks mental capacity to decide about their own personal information, the Mental Capacity Act 2005 Code of Practice states that certain other people may be able to request access to that information. This would be somebody with a lasting power of attorney, an enduring power of attorney or who is a deputy appointed by the Court of Protection.

8. Information about deceased people

Sometimes requests are made in relation to deceased people. For example, a family may suspect a safeguarding issue preceded or led to a relative's death. Although the Data Protection Act 1998 does not apply to information relating to deceased persons, there may be a need or legal justification for enduring confidentiality of a deceased person's record. However, any such requests would therefore come under the Freedom of Information Act 2000 (with due regard to the Data Protection Act) or sometimes under the Access to Health Records Act 1990 (this gives a right of access to information by a dead patient's representative or any person who might have a claim arising out of the patient's death). In any event, it may be advisable to seek advice from your legal or information governance teams in regards to these requests.

Appendix B to this document sets out further details regarding the legal basis for sharing information for specific purposes.

Although the DPA does not apply to deceased individuals, when considering whether to disclose information in relation to a deceased individual, the common law duty of confidence and Human Rights Act 1998 must be considered.

9. What information does each signatory need to share?

This Information Sharing Agreement has been produced to include a number of both operational and review purposes.

These include:

- Information about children and families that indicates reasonable cause to suspect children suffering or likely to suffer significant harm under section 47 of the Children Act 1989

- Information about children and families that indicates a child is in need under Section 17(10)

- For the purposes of Early Help and prevention to improve outcomes for children and young people at all stages of their development

- For the purposes of the prevention and detection of Child Sexual Exploitation (CSE) offences by the multi-agency team hosted by Leicestershire Police

- For the purposes of information sharing in response to protecting children at risk of, or the victims of, Female Genital Mutilation (FGM)

- For the purposes of the Leicester and Leicestershire & Rutland Local Safeguarding Children Boards under their duty to conduct Serious Case Reviews (SCRs), other review and audit processes.

For more information see Appendix B.

The following are the types of data that may be proportionate, relevant and necessary to share between partners for the purposes of safeguarding children:

Examples of the data that may be required
Name(s) and Alias
Dates of Birth and Dates of Death (if applicable)
Current Address and Previous Addresses
Contact information and Next of Kin
Family information regarding siblings
Information on contacts with service/team
Outcomes of contacts
Names of key workers/staff involved
Alleged perpetrator and their relationship to the victim
Health information (GP/Health Workers involved)
Photos of injuries sustained
Child Protection Plans and associated documentation
Any other relevant information (relevance must be evidenced)

A thought process to support the reason for requesting any personal information ensures that information is only requested where there is a justifiable need, rather than “nice to know”.

When a professional has made the decision to share information s/he must –

- Ensure information shared is necessary for the purpose for which it is being shared

- Understand the limits of any consent given, especially if the information has been provided by a third party
- Distinguish fact from opinion
- Share the information only with the person or people who need to know
- Check that the information is accurate and up-to-date
- Share the information in a secure way
- Establish whether the recipient intends to pass it on to other people, and ensure the recipient understands the limits of any consent that has been given
- Ensure that the person to which the information relates (or the person who provided the information) is informed that you are sharing information where it is safe to do so.

10. Who will own the information?

The Chief Executive/Officer of the agency/organisation which originally holds the personal information is the Data Controller. Once that information is shared with another partner to this ISA, the Data Controller of the agency/organisation receiving the information becomes the Data Controller on receipt; s/he will be responsible for ensuring that the information is held and used securely in accordance with this purpose, relevant legislation and this Information Sharing Agreement. No data will be forwarded on to a third party or sub-contractor without the express written permission of the original data controller.

11. Health and social care information: Caldicott guardians

Department of Health guidance states that NHS bodies and local authorities should appoint “Caldicott guardians” (DH, 1992, 2002a). The role of these guardians is to develop local protocols and perform a number of other functions in order to ensure that 6 principles are adhered to in relation to the handling of **personal** information.

The Caldicott Principles (Revised September 2013)

Principle 1. Justify the purpose(s) for using confidential information

> 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.

Principle 2. Don't use personal confidential data unless it is absolutely necessary

> Personal confidential data items should not be included unless they are 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).

Principle 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 is transferred or accessible as is necessary for a given function to be carried out.

Principle 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.

Principle 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.

Principle 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.

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.

12. How are you going to keep information accurate?

It is the responsibility of each partner agency to ensure as far as possible the information they supply is accurate. Care should be taken when checking the accuracy of the information to be shared and the details of the person or agency the information will be shared with.

13. Security of Information

If telephone calls are used to share information you must ensure you are disclosing to the authorised person and have the correct number.

The most secure electronic method available and agreed within your own agency should be used. This should be using GCSx email where possible.

GCSx stands for Government Connect Secure Extranet. It is a secure private Wide-Area Network (WAN) which enables secure interactions between connected local authorities and agencies/organisations.

GCSx is connected to the Government Secure Intranet (GSI), which also enables secure interactions between local authorities and central government departments and national bodies. GCSx provides a range of connectivity options to enable

access to the GSI network and its hosted services; GCSx does not use the Internet or any other public networks.

GCSx provides secure access from connected local authorities to many other secure networks such as:

- Government Secure Extranet (GSX)
- Government Secure Intranet (GSI)
- National Health Service (NHS.net)
- Criminal Justice Extranet (CJX)
- Police National Network (PNN).

When sending out emails, faxes or correspondence containing confidential information practitioners should follow their agency policies and procedures. In some agencies such as the Police there are restrictions on the methods that can be used to share confidential information.

Please see Appendix C for further information on information sharing, storage and destruction methods.

14. How long will the information be kept?

Each agency/organisation which has received information referred to in this agreement will have their own policy which says how long they will keep different types of information. Please refer to individual agencies' policies for details.

E.g.
'X' Agency/Organisation will keep the shared information for …… /or a period of ……. years.

'Y' Agency/Organisation will keep the shared information for …… /or a period of ….. years.

15. How will we keep information secure?

Information will then be held securely within each agency's/organisation's electronic file structure in accordance with their own organisational security measures.

16. What if we want to use the information for something else?

If any agency/organisation wishes to use the information which they have been given under this agreement, for any purpose other than that in Section 2 above, they must first ask the agency/organisation which provided the information for their written consent to ensure compliance with the Data Protection Act 1998.

17. What do we do if information is lost, disclosed, misused, etc?

If any information which is shared under this agreement is lost, stolen or disclosed to someone who should not have seen it, this is not only a breach of confidentiality but is likely to be a breach of the Data Protection Act (for which the Data Controller can be fined up to £500,000). If the information is deliberately accessed and/or disclosed by someone who is not entitled to see or use it, this person may have committed a

criminal offence under the Data Protection Act 1998 or the Computer Misuse Act 1990. Information may be deleted when it should have been kept. These are all information breaches.

It is important that the agency/organisation(s) which provided the information are told as soon as possible so that they can risk assess what has happened – they may need to tell individuals what has happened to their information and they may need to tell the Information Commissioner. An investigation may have to be undertaken by the Police (to determine whether any criminal investigations are required) or the Information Commissioner so evidence, including audit trails and printouts, can be recovered.

All partners involved in the breach will investigate and record the breach and the outcome of the breach will be circulated to the partners involved.

The agency/organisation where the breach occurred may need to do an internal investigation and this may lead to disciplinary action or identifying processes which need to be changed.

Each agency/organisation should provide contact details of the post in their agency/organisation who should be informed if an information breach occurs in the table below.

Agency/Organisation	Post	Email	Telephone

18. How will you check if your colleagues are complying with this agreement and if it is still current?

The Local Safeguarding Children Boards, on behalf of the agencies who are party to this agreement, will review this agreement within 2 years of commencement of this ISA. A self-assessment by agencies of compliance will feature as a part of the yearly Section 11 audit undertaken by the LSCBs.

19. What happens if there is a major security breach?

Any agency/organisation can suspend this ISA for 45 days if security has been seriously breached. This should be in writing and provide evidence of what went wrong. A representative from each agency/organisation should meet as soon as possible (no longer than 14 days) to carry out a Risk Assessment and Resolution meeting.

Termination of, or withdrawal from, this ISA should be in writing to all other partner agencies/organisations, giving at least 30 days' notice.

20. What do we do if the data subject asks for information which we receive under this ISA?

<u>Data Protection Act 1998</u>

You may receive a request under the Data Protection Act 1998 by the data subject. In Leicester, Leicestershire and Rutland, it has been agreed that when an agency/organisation receives a request for information, which has been shared under this ISA, the agency/organisation that receives the request will tell the agency/organisation which provided the information and ask for their views about the disclosure of the information so this can inform the decision making process.

21. Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIR)

All recorded information held by public authorities is subject to the provisions of FOIA and EIR. You may receive a request under the FOIA or EIR. It has been agreed that when an agency/organisation receives a request for information which has been shared under this ISA, the agency/organisation which receives the request will tell the agency/organisation which provided the information and ask for their views about the disclosure of the information so this can inform the decision making process.

22. Who are the Responsible People in each agency/organisation?

Information sharing activity should be reviewed and approved by the agency's/organisation's legal/information security staff. Each agency/organisation should give details of the post which is responsible on a day to day basis for monitoring compliance with this ISA.

23. Who are the Appropriate Signatories in each agency/organisation?

Each partner should identify who is the most appropriate post holder within their agency to sign the ISA having taken account of their organisational policy and the fact that the signatory must have delegated responsibility to commit their agency/organisation to the agreement. Don't forget this is the person who is making the commitment on behalf of the agency/organisation that the conditions in this ISA will be complied with.

Each agency/organisation who is a signatory to this ISA will be asked to complete the table below which will identify the appropriate post holder to sign this agreement on behalf of their agency/organisation. In addition the agency/organisation will be asked to identify the post which is responsible on a day to day basis for monitoring compliance with this ISA.

Agency/Organisation:	
Person signing this Information Sharing Agreement	
Name:	
Role:	
Signature:	
Date:	
Responsible Person	

Post:	
Address:	
Tel:	
Email:	

VERSION CONTROL			
DATE	VERSION	COMMENTS & AMENDMENTS	BY WHOM
12.06.14	DRAFT V0.01	First Draft	Chris Tew & Janette Harrison
26.06.14	DRAFT V0.02	Additions in appendix	Chris Tew
01.07.14	DRAFT V0.03	To include link to LSCB Procedures/Consent for Early Support and further information on sharing information without consent. Amendment in red for consideration	Janette Harrison
09.07.14	DRAFT V0.04	Further consolidation work and website linking. Submitted for initial legal advice	Chris Tew
30.07.14	DRAFT V0.05	Following review by information security team, advice about GCSx included at Section 7. Examples of types of info shared at Section 2 added. Storage of information and Breaches of Security sections added	Chris Tew
24.09.14	DRAFT V0.06	Incorporating feedback from consultation UHL and Leicestershire Legal	Chris Tew
01.10.14	DRAFT V0.07	Incorporating feedback from consultation Leics Police	Chris Tew
12.11.14	DRAFT V0.08	New format following further input from Leicestershire Information Governance	Chris Tew
09.12.14	DRAFT V0.09	Comments and CSE additions	Janette Harrison
29.01.15	Draft V0.9.1	Updated following second consultation with amendments suggested by agencies	Janette Harrison/Chris Tew
03.02.15	V1.0	Completed version for distribution to agencies	Janette Harrison/Chris Tew
04.02.15	V1.01	Prevent section added	Chris Tew
27.05.15	V1.02	Further amendments added by Leicestershire Police	Ravi Nagra-Kumar/Angela Middleton
28.05.15	V1.03	Amended and Formatted. Sent to Police for agreement	Chris Tew
10.06.15	V1.04	Charities considerations added	Chris Tew
10.09.15	V2.00	Finalised following agencies signing	Chris Tew
5.10.16	V3.00	Glebe house project included	Chris Tew
18.1.17	V4.00	Diocese of Leicester included	Chris Tew

APPENDIX A

Principles for Action

Information sharing is vital to safeguarding and promoting the welfare of children and young people. A key factor in many Serious Case Reviews (SCRs) has been a failure to record information, to share it, to understand its significance and then take appropriate action.

The Government guidance "Information sharing advice for safeguarding practitioners 2015" highlights 7 golden rules for information sharing:

- 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.

Sharing Information: Questions for staff to ask

Is there a clear and legitimate purpose for sharing information?

Under Section 11 of the Children Act 2004 key people and bodies have the duty to make arrangements which ensure their functions are discharged with regard to the need to safeguard and promote the welfare of children. This extends to the member agencies of the LSCB and the services they commission. Information sharing is fundamental for complying with this statutory regulation.

Information sharing for statutory and non-statutory services must comply with laws relating to confidentiality, data protection and Human Rights.

Consent is not required from the subject of the information when an agency is required by law to share information or when a court makes an order for certain information or case files to be made available to the court. Such situations do not arise often but when they do practitioners must share information. A court order may be challenged by your agency/organisation but all other situations must be complied with by practitioners.

Exceptions to the requirement to consent

As a general rule, personal information shared in confidence should not be used or disclosed further without the consent of the individual.

Exceptions to the requirement for consent are rare and limited to legal requirements to disclose information, e.g. by Acts of Parliament or court orders; disclosures permitted by regulations made under section 251 of the NHS Act 2006 (previously known as section 60 of the Health and Social Care Act 2001); or where there is a public interest justification for breaching confidentiality such as a serious crime, including murder, rape or child abuse.

Does the information enable a living person to be identified?

Information which has been made anonymous can be shared. However, information which identifies an individual, or could identify a person living when considered with other information, is personal information and is subject to Data Protection Act 1998. There are issues of confidentiality in relation to deceased individual's records: please see Information Commissioner's website here for further details.

Is the information confidential?

Not all information is confidential. Confidential information is data of some sensitivity which is not already lawfully in the public domain or readily available from another public source and has been shared in a relationship where the person giving the information understood that it would not be shared with others.

Information which is not confidential may generally be shared where necessary for the legitimate purposes of statutory and preventative work.

Confidence is only breached where the sharing of confidential information is not authorised by the person who provided it or to whom it relates. If the information

was provided on the understanding that it would be shared with a limited range of people or for limited purposes then sharing in accordance with that understanding will not be a breach of confidence. Similarly, there will not be a breach of confidence where there is explicit consent to the sharing.

Information can be lawfully shared, even if this has not been authorised, if this can be justified in the public's interest: for example, to protect a child or someone else from harm or to promote the welfare of a child to prevent crime and disorder.

Who do you owe confidentiality to?

The duty of confidentiality is owed to the individual to whom the information relates and to the person who has provided the information on the understanding it is to be kept confidential.

Do you have consent to share?

As a matter of good practice, practitioners should inform children, young people and families about their service's policy on how information will be shared and seek their consent. If there is significant change in the way the information is to be used, or a change in the relationship between the agency and the individual, consent should be sought again. It must be remembered that individuals have a right to withdraw or limit consent at any time.

Informed consent means that the person giving consent needs to understand why information would be shared, who will see their information, what it will be used for and the implications of sharing that information. We seek to promote a climate of openness and honesty with children and families where, in the main, informed consent is obtained at the start of intervention in children's lives and gained again where circumstances alter – for example, where an agency wishes to make a referral of a child with additional needs, or a child in need, to another agency.

Whose consent should be sought?

Seeking consent can at times pose difficult dilemmas. The principle should always be one of openness with both parents and children. Practitioners, wherever possible, should seek to gain the consent of parents and children. Adults (but also young people over the age of 16) are presumed to have the capacity to give or withhold their consent to sharing of confidential information, unless there is evidence to the contrary under the Mental Capacity Act 2005.

A child, who is able to understand and make their own decisions, is able to give or refuse consent to share information. Every case should be assessed to gauge a child's understanding of consent, explaining the information to the child in a way which is suitable for the child's age and likely understanding and through using their preferred method of communication.

Capacity to give consent is a “functional test” and is not dependant on age. Generally children aged over 12 may be expected to have sufficient understanding. However, younger children may also have enough understanding while some older children will not. When assessing children for “sufficient understanding” practitioners should consider whether the child has a reasonable understanding of what

information might be shared, the main reason(s) for sharing it and the implications of sharing or not sharing the information.

Practitioners should address whether a child can:

- 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: are they constantly changing their mind?

Where a child cannot consent, one person with parental responsibility should be asked to consent on behalf of the child. In these circumstances it remains important that practitioners seek the child's views as far as possible. When seeking parental consent, practitioners should ensure proper consideration is given to whose consent to seek. For example, where parents are separated, consent should be sought from the parent with whom the child resides.

Where a child is able to give informed consent, the practitioner must consider their consent or refusal even where a parent disagrees. In such circumstances the practitioner must encourage the child to discuss the issue with their parents and agree how this will be managed. Practitioners must not withhold any service on the condition that parents are informed.

When consent should not be sought

Wherever possible practitioners should seek consent to share information at their first contact whenever they are concerned about a child with additional needs, a child in need or a child in need of protection. There may, however, be some circumstances where they should not seek consent initially but even so should obtain consent when it is appropriate to do so.

For example, if doing so would:

"place a person (the individual, family member, yourself or a third party) at increased risk of significant harm if a child, or serious harm if an adult; or

prejudice the prevention, detection or prosecution of a serious crime; or

lead to an unjustified delay in making enquiries about allegations of significant harm to a child, or serious harm to an adult"

Information Sharing: Guidance for Practitioners and Managers (2008).

Can I share information when I cannot obtain consent or consent is refused?

Where information is confidential and consent is refused, that should be respected unless in the practitioner's professional judgment, on the facts of the case, there is justification for sharing information.

Where consent cannot be obtained to share information or consent is refused, or where seeking it may undermine the prevention, detection or prosecution of a crime, the practitioner must judge from the facts whether there is enough public interest. A concern in relation to protecting a child from significant harm, promoting the welfare of children, protecting adults from serious harm or preventing crime and disorder are all well within public interest.

Sharing confidential information without consent will normally be justified in the public interest:

(a) When there is evidence or reasonable cause to believe that a child is suffering, or is at risk of suffering, significant harm

(b) When there is evidence or reasonable cause to believe that an adult is suffering, or is at risk of suffering, serious harm

(c) To prevent significant harm to a child or serious harm to an adult, including through the prevention, detection and prosecution of serious crime.

Practitioners must decide whether sharing information is a necessary and proportionate response to the need to protect the child in question. The decision making process must weigh up what might happen if the information is shared against what might happen if it is not shared. It is important to note that a lack of information sharing is a consistent theme within Serious Case Reviews.

What information may be shared?

It is necessary to show proportionality when information is shared, i.e. that a fair balance has been struck between the individual rights of the person and the relevant justification.

Appendix B

This appendix provides specific information regarding the purposes for sharing information mentioned in the previous section “Legal Basis – What law allows you to share this information?”

Practitioners who are unsure of their information sharing responsibilities should be mindful of the need to seek supervision to validate their decision making.

Section 17 Children in need

Section 17 referrals are usually made with parent/carer consent but consent is not required in cases where failure to share information could result in the situation deteriorating.

Children's Social Care will accept a referral about a child regardless of whether consent has been given.

Children's Social Care will firstly assess the child to see if the child is in need (Section 17, Children Act 2004) of a service and or is in need of protection (Section 47, Children Act 2004).

Information must be collected from agencies who know the child for these decisions to be made and consent is not required for this activity. These are statutory requirements under the Children Act and thus covered by the Data Protection Act 1998, Schedules 2 and 3.

Consent is needed for a service to be offered. So where a child is clearly a “child in need” of a service then the first action for Children's Social Care must be to obtain consent, unless of course it has been obtained earlier in the process.

Further guidance for General Practitioners is available from:

Safeguarding Children and Young People: The RCGP/NSPCC Safeguarding Children Toolkit for General Practice 2014

Referral to specialist Early Help/Common Assessment Framework (CAF) services

Early Help referrals are usually made with parent/carer consent but consent is not required in cases where failure to share information could result in the situation deteriorating.

Section 47 Child Protection

Where a local authority is conducting enquiries under Section 47, the following agencies/organisations are under a statutory duty to assist the local authority with those enquiries (in particular by providing relevant information and advice) if called upon by the authority to do so:

- Any local authority

- Any Local Housing Authority
- The National Health Service Commissioning Board
- Any Clinical Commissioning Group
- Any National Health Service Trust or NHS Foundation Trust.

Whilst it is good practice to share with families your intention to make a referral to Children's Social Care about their child's welfare, it is not a prerequisite. In some circumstances you should not inform the family about the referral: for example, where evidence of abuse is likely to be removed or where a child will be placed at increased risk when parents have this knowledge.

Therefore, as a general rule in safeguarding children, consent is not required for Section 47 referrals where a child is considered at risk or is thought to have suffered significant harm. Nevertheless, consent should be sought unless to do so would increase harm to the child.

Adults at risk

Practitioners working in children services need to be mindful of the requirements to alert and, if necessary, share information with Adult Social Care of any parent or carer who is at risk of abuse. This may also apply to any other adult at risk as defined by the Care Act 2014.

Please see here for further information regarding the Care Act 2014.

For further information, refer to the Leicestershire & Rutland Adult ISA.

Information sharing for the purposes of preventing or detecting crime

This is outlined in Section 29 of the Data Protection Act 1988 and includes:

(1) Personal data processed for any of the following purposes –

(a) The prevention or detection of crime

(b) The apprehension or prosecution of offenders

(c) The assessment or collection of any tax or duty, or of any imposition of a similar nature, are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

(2) Personal data which –

(a) Are processed for the purpose of discharging statutory functions

(b) Consist of information obtained for such a purpose, from a person who had it in his possession for any of the purposes mentioned in subsection (1), are exempt from the subject information provisions to the same extent as

personal data processed for any of the purposes mentioned in that subsection.

(3) Personal data are exempt from the non-disclosure provisions in any case in which –

(a) The disclosure is for any of the purposes mentioned in subsection (1)

(b) The application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.

(4) Personal data in respect of which the data controller is a relevant authority and which –

(a) Consist of a classification applied to the data subject as part of a system of risk assessment which is operated by that authority for either of the following purposes –

i. The assessment or collection of any tax or duty or any imposition of a similar nature
ii. The prevention or detection of crime, or apprehension or prosecution of offenders, where the offence concerned involves any unlawful claim for any payment out of, or any unlawful application of, public funds

and

(b) Are processed for either of those purposes

(c) Are exempt from section 7 to the extent to which the exemption is required in the interests of the operation of the system.

(5) In subsection (4) – "public funds" includes funds provided by any [F1 EU] institution; "relevant authority" means –

(a) A government department
(b) A local authority
(c) Any other authority administering housing benefit or council tax benefit.

Prevent

Prevent is 1 of the 4 elements of CONTEST, the government's counter-terrorism strategy. It aims to stop people becoming terrorists or supporting terrorism.

The Prevent strategy:

- Responds to the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views
- Provides practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support
- Works with a wide range of sectors (including education, criminal justice, faith, charities, online and health) where there are risks of radicalisation that we need to deal with.

The strategy covers all forms of terrorism, including far-right extremism and some aspects of non-violent extremism. However, we prioritise our work according to the risks we face.

The Home Office works with local authorities, a wide range of government departments and community organisations to deliver the Prevent strategy. The Police also play a significant role in Prevent, in much the same way as they do when taking a preventative approach to other crimes.

Further information can be obtained from the Leicester Prevent website here.

Serious Case Reviews

Regulation 5 of the Local Safeguarding Children Boards Regulations 2006 sets out the functions of LSCBs. This includes the requirement for LSCBs to undertake reviews of serious cases in specified circumstances. Regulation 5(1)(e) and (2) set out an LSCB's function in relation to Serious Case Reviews, namely:

5(1)(e) Undertaking reviews of serious cases and advising the authority and their Board partners on lessons to be learned.

(2) For the purposes of paragraph (1) (e) a serious case is one where:

(a) Abuse or neglect of a child is known or suspected

and

(b) Either – (i) the child has died; or (ii) the child has been seriously harmed and there is cause for concern as to the way in which the authority, their Board partners or other relevant persons have worked together to safeguard the child.

Other LSCB review and audit purposes and the statutory duty to provide information

Section 14B Children Act 2004 provides that if the LSCB requests a person or agency/organisation to supply information to the Board then that agency/organisation is under a statutory duty to comply with that request provided that:

- The request is made to assist the Board to perform its functions
- The request is made to a body who the Board considers are likely to have relevant information

and

- The information requested relates to a person in respect of whom the agency/organisation exercises a function / engages in activity
- To the agency/organisation to whom the request is made
- To the functions/activities of the agency/organisation to whom the request is made.

We would need to be mindful of general HRA duties to ensure that we only request (and the agency/organisation only provides) information that is proportionate to the request – so that would require the agency/organisation to filter and remove material that is irrelevant for the purposes of the review.

What are the LSCB functions?

The LSCB Regulations 2006 set out the functions of the LSCB which include undertaking SCRs. The Regulations also confer the power on the Board to engage in any other activity that facilitates or is conducive to the achievement of its objectives.

The relevant statutory guidance provided in Working Together 2013 states:

Chapter 1 sets out how effective sharing of information between professionals and local agencies is essential for effective service provision. Every LSCB should play a strong role in supporting information sharing between and within agencies/organisations and addressing any barriers to information sharing. This should include ensuring that a culture of information sharing is developed and supported as necessary by multi-agency training.

In addition, the LSCB can require a person or body to comply with a request for information. This can only take place where the information requested is for the purpose of enabling or assisting the LSCB to perform its functions. Any request for information about individuals must be necessary and proportionate to the reasons for the request. LSCBs should be mindful of the burden of requests and should explain why the information is needed.

And:

Each local framework should support the work of the LSCB and their partners so that:

- Reviews are conducted regularly, not only on cases which meet statutory criteria, but also on other cases which can provide useful insights into the way agencies/organisations are working together to safeguard and protect the welfare of children
- Reviews look at what happened in a case, and why and what action will be taken to learn from the review findings
- Action results in lasting improvements to services which safeguard and promote the welfare of children and help protect them from harm

and

- There is transparency about the issues arising from individual cases and the actions which agencies/organisations are taking in response to them, including sharing the final reports of Serious Case Reviews (SCRs) with the public.

In addition:

LSCBs should also conduct reviews of cases which do not meet the criteria for an SCR, but which can provide valuable lessons about how agencies/organisations are working together to safeguard and promote the welfare of children.

Although not required by statute, these reviews are important for highlighting good practice as well as identifying improvements which need to be made to local services. Such reviews may be conducted either by a single agency/organisation or by a number of agencies/organisations working together. LSCBs should follow the principles in this guidance when conducting these reviews.

For example, one such review type is the "Appreciative Inquiry" which does not meet the criteria for a SCR but, in accordance with WT as set out above, it is recognised that the LSCB should also conduct reviews of cases which do not meet the criteria for a SCR but which can provide valuable lessons about how agencies/organisations are working together to safeguard and promote the welfare of children. Although not required by statute, these reviews are important for highlighting good practice and identifying improvements which need to be made to local services; such reviews can be single or multiple agency reviews and, if the latter, the statutory guidance provides that the WT principles should be followed.

So, whilst the "Appreciative Inquiry Review" is not required by statute, it still falls within the LSCB statutory functions set out in the Regulations as it is permitted by statute and is promoted and encouraged by the statutory guidance. The LSCB, therefore, is exercising its functions under regulation 5(3) if it undertakes an Appreciative Review (as long as the review is conducive to meeting the objectives set out in WT, i.e. the LSCB considers that lessons could be learnt about inter-agency working etc.). It follows from the above that this is an LSCB function and, therefore, S14B of the Children Act applies to any request for information.

Audits conducted as part of the core business of the Local Safeguarding Children are also subject to the above criteria.

Female Genital Mutilation (FGM)

FGM is a form of child abuse and violence against women and girls and, therefore, should be dealt with as part of existing child and adult protection structures, policies and procedures. Further details regarding FGM can be found in the Government Multi-Agency Practice Guidelines for FGM, which are available here.

Child Sexual Exploitation

Information may be shared under this agreement for the following purposes:

- To facilitate best practice in order to provide a more integrated and coordinated approach to identified victims of Child Sexual Exploitation

- To inform multi-agency actions to prevent abuse occurring, disrupt perpetrator activity and secure evidence to support prosecutions. This may involve sharing intelligence gathered through the course of routine work: for example, if a cohort of young people or vulnerable adults are found to have similar

sexually transmitted infections or professionals involved are concerned about relationships in an area that could be potentially coercive

- To provide information, which may be anonymised if more appropriate, on areas or cohorts of concern

- To establish the potential involvement of partner agencies with identified victims/perpetrators

- For sharing information with partner agencies that may be providing services to the victim, their family or perpetrator of any actions taken

- To provide information to partners in other local authority areas so that links between potential abusers are recognised and actioned.

In adopting this partnership approach, partners will work together to identify, support and safeguard children and young people and vulnerable adults who are vulnerable to sexual exploitation from those who are intent on abusing them.

Acknowledgement: Barnsley Safeguarding Children Board (21 March 2014)

Private Fostering

LLR Procedures 2.9 Children Living Away From Home

A private fostering arrangement is essentially one that is made without the direct involvement of a local authority for the care of a child under the age of 16 (under 18 if disabled) by someone other than a parent or close relative for 28 days or more. A close relative is defined as "a grandparent, brother, sister, uncle or aunt (whether of the full blood or half blood or by marriage or civil partnership) or step-parent". Becoming aware that a child is being privately fostered requires vigilance by practitioners. Teachers, health professionals (particularly GPs and Health Visitors) and other professionals should notify the appropriate Duty Team of a private fostering arrangement where they are not satisfied that the arrangement has been, or will be notified. The family are to be advised to notify the local authority about the arrangement.

Early Help/Support

The concept of Early Help and prevention reflects the widespread understanding that it is better to identify and deal with problems early rather than to respond when difficulties have become acute and require action by more intensive services.

The purpose of Early Help and prevention is to improve outcomes for children and young people at all stages of their development: from pre-birth, through the early years stage, throughout their school careers and into their transition to adulthood. Difficulties may emerge at any point throughout childhood and adolescence.

Early Help and prevention is about how universal and targeted services are coordinated to identify, reduce and prevent specific problems from getting worse or becoming entrenched. Early Help and prevention gives families the opportunity to

address their problems, ensuring children stay safe and achieve their full potential. Signed consent is required when referring for Early Support/CAF.

The documents completed for referral to Early Support/CAF services are to make clear the following:

- That the information individuals consent to being shared will be treated as confidential and will not be shared without their agreement and consent unless there is a need to by law to either (a) prevent harm occurring or (b) to prevent the law being broken

- The signatory is to include information that reflects the following statement:

  > "I have had the reasons for Early Support/CAF explained to me and I understand those reasons. I agree to my information being shared in order that the work can take place and services to help and support me can be provided. The information will not be used for any other purpose."

- Where consent for Early Support is refused, professionals are to continue to support and assess to determine whether without the provision of early support the child/children's circumstances will meet the criteria for child in need or child protection.

Appendix C

Sharing & Destruction Methods	Security Requirements
Agencies/Organisation Data Network (e.g. internal email)	Recommend passwording attachments for sensitive personal data in case it is sent to wrong email address. No personal data in subject title or sensitive personal data in body of email. Use of GCSx network where available Recommend turning off autofill of address field
Email between partners	Passwording attachments for sensitive personal data in case they are sent to wrong email address. No personal data in subject title, or sensitive personal data in body of email To/from Police: restricted or sensitive personal data only to emails using PNN, GSI, CJSM or MOD secure addressing conventions or via GCSx and PSN connections To/from NHS: secure transfer as agreed with health partners (currently under discussion county-wide due to new health arrangements – to be updated when agreed)
Laptops, removable media, USB, etc.	Must be owned by the employer and encrypted. No personal information from any of the agencies/organisations in this ISA is to be loaded to personally owned removable media
Electronic storage of information	Has the application where it will be stored been pen tested? In other words, could someone hack into it? Check with your IT department How will access to the information be restricted? Please say how this will be done Is there an audit trail which will show

	who has accessed a record?
Vetting/clearance of staff	Have the staff who will receive and access the information been vetted?
Internal and public telephone network	May be used
Mobile telephone (voice and text)	Digital cell phones may be used Only use analogue cell phones if operationally urgent, use guarded speech and keep conversation brief
Fax	Note faxes are legacy technology and are NOT to be used unless there is no alternative. If no alternative, check recipient is on hand to receive Send cover sheet first and wait for confirmation before sending
Storage of papers	Protected by one barrier, e.g. a locked container within a secure building/room. Locked filing cabinet for storage if home working
Disposal of papers	Use secure waste sacks if agency/organisation has system in place and make sure they are secure when left unattended or collected for destruction Shred personal information if it is very sensitive
Disposal of magnetic media	All types of discs and other storage devices – dismantle and destroy by disintegrating, pulverising, melting or shredding then dispose with normal waste/recycling following destruction
Movement within agency/ organisation via internal mail	In a sealed envelope with protective marking shown
Movement between partner agencies	By post or courier in a sealed envelope
Movement between workplace and home/mobile office	On encrypted memory stick or lockable briefcase. Locked filing cabinet for storage if home working

* If agencies/organisations do not find it possible to apply the appropriate security this should be discussed with the originator.