**Hertfordshire Family Safeguarding Service: Guide to information sharing**

This Guide has been written to complement the Hertfordshire Family Safeguarding Service Information Sharing Agreement and Protocol, and provides further details on information sharing relating to that agreement. It will be reviewed annually in line with the agreed review timescales of this Agreement which has been signed by the following organisations:

Hertfordshire County Council:
Hertfordshire Constabulary
Bedfordshire Northamptonshire Cambridgeshire & Hertfordshire Community Rehabilitation Company (BeNCH),
Hertfordshire Community NHS Trust
Hertfordshire Partnership University NHS Foundation Trust
National Probation Service?
CRI Ltd

**Agreement start date: December 2015**

**Agreement review by date: December 2018**

**Introduction**
In order to ensure that safeguarding decisions are made with timely, necessary and proportionate interventions and support, decision makers require full information concerning children, their parents, carers and their circumstances to be available to them. Information viewed alone or in silos is unlikely to give the full picture or identify the true risks.

All relevant information from various agencies involved in their care or support, needs to be available and accessible in one place. The ethos and practice underpinning Family Safeguarding helps ensure this and aids communication between all partners. By ensuring all active partners have the ability to share information, in a timely manner it will help to identify those who are subject to, or likely to be subject to harm, and provide support to vulnerable individuals with the aim of reducing harm and improving the welfare of children and vulnerable adults

Information should only be shared by partners for the purposes of safeguarding and promoting the welfare of children and vulnerable adults and for the prevention and detection of related crime.

HM Government advice on Information Sharing (March 2015) states "***Sharing information is an intrinsic part of any front-line practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. It could ensure that an individual receives the right services at the right time and prevent a need from becoming more acute and difficult to meet. At the other end of the spectrum it could be the difference between life and death."***

Poor or non-existent information sharing is a factor repeatedly flagged up as an issue in Serious Case Reviews carried out following the death of, or serious injury to, a child.

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. No practitioner should assume that someone else will pass on information which may be critical to keeping a child safe.

A public authority such as HCC has some legal power enabling it to share the information. We must consider on a case by case basis whether information will be shared with or without consent, through considering what is reasonable, necessary and proportionate.

**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.

**Definitions**

Personal Information/Data is:

- Information/Data which relates to a living, individual who can be identified from the data or other data/information that HCC holds
- Could be single elements or a combination e.g. names, addresses, occupation, date of birth etc.it could also include opinions about them and intentions towards them.
-

Sensitive Personal Information/Data is:

- Physical or mental health, racial or ethnic origin, political opinions, TU membership, sexual life, criminal allegations or record.

## Principles

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

### Necessary and proportionate

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

### Relevant

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

### Adequate

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

### Accurate

Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

### Timely

Information should be shared in a timely fashion to reduce the risk of harm. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore harm to a child. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

### Secure

Information should be shared in the most secure way available. Practitioners must always follow their organisation's policy on security for handling personal information

### Record

Information sharing decisions should be recorded whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with each organisation's own retention policy.

**What Information can I share?**
Share the information which is necessary for your purpose. It may not be necessary to give all agencies access to all the information you hold. Make sure what you provide is up to date, accurate and relevant.

**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.

**When?**
Is there a clear and legitimate purpose for sharing information?

• Yes – see next question

• No – then do not share information

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

• No – you can share but should consider how

Is the information confidential?
• Yes – see next question

• No – you can share but should consider how

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

• No – see next question
Is there another reason to share information such as to fulfil a public function or to protect the vital interests of the individual?

• Yes – you can share but should consider how

• No – do not share

**Who?**

- Which agencies need to be involved in the sharing?

- Who do we need information about in order to make the decision – child, parent, carer, others? Is it sensitive personal information? Do we have their consent?

**How?**

- Ensure you are giving the right information to the right person, and that it is shared securely.
- Identify how much information to share

- Distinguish fact from opinion

- Ensure that you are giving the right information to the right person
- Inform the individual that the information has been shared if they were not aware of this, as long as this would not create or increase risk of harm

**Consent to share information**

Check you have consent from all people whose information is to be shared unless the safeguarding concerns put the child at risk of significant harm or would prevent the child from being harmed. Ensure information shared is relevant and proportionate.

Where possible, consent should be obtained by the Partner organisation before individual cases are discussed by Family Safeguarding teams. In these cases, individuals will have an understanding and expectations of how their information is going to be used, with whom and why.

Where consent has not been obtained, reasons for this must be documented by the relevant Partner. The rule of proportionality should be applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject.

Where sensitive personal information is being shared explicit consent is expected, this may be written e.g. consent form or a clear record of verbal consent obtained stating the date, time and what information is to be held/shared.

In some cases, the work of the Family Safeguarding Service might be obstructed if Partners were to seek consent. In such cases the disclosing Partner must consider other lawful basis for processing the information.

The decision whether or not to share information must be recorded by the partner agency which makes that decision.

**Consider the following before sharing information - *if in doubt seek advice from a manager***

<u>Consent</u>

Do you have consent to share this information for this purpose? Consent is particularly important for sensitive personal information. The Privacy Notice (a statement that indicates consent to hold and share information see consent form) relating to the collection of information should identify the purposes for which it was collected. Does this say it would be shared? Otherwise consent should be obtained wherever possible before sharing information.

<u>Partial Consent</u>
Where consent has been given to share information with some, but not all, agencies, does this include the agency you want to share it with? If you do

have consent, then the paragraph above applies. If you do not have consent, then the paragraph below applies.

Sharing without consent

If you are not seeking consent, the reason must be proportionate and you must weigh up the important legal duty to seek consent and the damage that might be caused by sharing the information. This should be balanced against the type and extent of any harm that might be caused (or not prevented) by seeking consent.

It is good practice to obtain consent before sharing information. If consent is not obtained, the decision should always be reasonable, necessary and proportionate, and should always be recorded together with the rationale.

If the need to share is urgent, and seeking consent will lead to unjustified delay in making enquiries about allegations of significant harm to a child, or if safeguarding is paramount, take immediate action and share the information without consent, but remember to record the reason for the decision.

Sharing information when consent has been refused

There may be times when consent is sought and refused. This does not mean that information cannot be shared. The refusal of consent should be considered in conjunction with other concerns and, if it is considered justifiable, then information can and **MUST** be shared. If professionals consider it justifiable to override the refusal in the interests of the welfare of the child then they can do so. This decision must be proportionate to the harm that may be caused by proceeding without consent.

**Public Interest**

It is possible to disclose personal information without consent if this is in the defined category of “Public Interest”. The principles of the DPA [Section 2 above] would still apply in such cases.

The ***Public Interest Criteria*** include the:

- Protection of vulnerable members of the community
- Administration of justice
- Maintaining of public safety
- Apprehension of offenders
- Prevention of crime and disorder
- Detection of crime

When judging the public interest, it is necessary to consider the following:

- Is the intended disclosure proportionate to the intended aim?
- What is the vulnerability of those who are at risk?
- What is the impact of disclosure likely to be on the individual to whom the shared information pertains?
- Is there another equally effective means of achieving the same aim?

- Is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public?
- Is it necessary to disclose the information, to protect others?

***The rule of proportionality should be applied to ensure that a fair balance is achieved between the public interest and the rights of the individual's information.***

**What is the Legal Framework that supports information sharing?**

The main legal framework relating to the protection of personal information is set out in:

- The Human Rights Act 1998, which incorporates Article 8 of the European Convention on Human Rights (ECHR), including the right to a private and family life
- The common law duty of confidentiality
- The Data Protection Act 1998, covering protection of personal information

There is no general power to obtain, hold or process information and there is no statutory power to share information. Where information is held it should be processed in accordance with the Data Protection Act principles.

However, some Acts of Parliament do give statutory public bodies express or implied statutory powers to share information under some circumstances. There are a number of pieces of legislation. Some of these are relevant to all members of the Family Safeguarding Teams. Others relate to specific organisations.

Data should only be shared between Family Safeguarding team members for the purposes of safeguarding children; promoting the welfare of children and vulnerable adults who are part of their family and for the prevention and detection of related crime***.***

Legislation allows the lawful sharing of personal information and is covered in this guide using the following legislative frameworks.

**Data Protection Act (DPA) 1998:**
The principles of the DPA 1998 provide a framework within which to consider the lawful basis for sharing information under this agreement. Details of the Data Protection Act Key Principles are attached to this guidance as Appendix 1.

Each partner agency may have a different reason for holding and processing the information it needs to fulfil its legal duties. Some common considerations have been included here, but it is impossible to cover all possible situations. Partner agencies must obtain their own assurance and be satisfied that they have a lawful basis for sharing the information they hold.

Partner agencies must be familiar with and apply the Hertfordshire Safeguarding Children Board (HSCB) guidance on information sharing and confidentiality.

**DPA** Section **29**
This section provides certain exemptions when personal information is used for the prevention and detection of crime and/or for the apprehension and prosecution of offenders. For example, telling individuals how their information will be processed or shared could prejudice the purpose. Note that information processed for this purpose is exempt from disclosure in response to a Subject Access Request.

**Children Act 2004**
Sections 10 and 11 of the Children Act 2004 place obligations upon specified agencies including local authorities, police, clinical commission groups and NHS England to co-operate with other relevant partners in promoting the welfare of children and also ensuring that their functions are discharged having regard to the need to safeguard and promote the welfare of children. The Act sets out the specific agencies for s10 and s11 – if in doubt check.

Section 10 and 11 of the Children Act 2004 create a 'permissive gateway' for information to be shared in a lawful manner. Such information sharing must take place in accordance with statutory requirements pertaining to the disclosure of information namely the Data Protection Act 1998, the Human Rights Act 1998 and the Common Law duty of confidentiality.

The Act, although amended by the Health and Social Care Act 2012, does not provide a basis for processing by non-Public Sector bodies, i.e. healthcare providers that are not NHS Trusts or NHS Foundation Trusts, charities, or private providers.

The Act emphasises the importance of safeguarding the welfare of children by stating that relevant partner agencies, must ensure that functions are discharged having regard to the need to safeguard and promote the welfare of children.

The Act also states that they must make arrangements to promote co-operation between relevant partner agencies to improve the well-being of children in their area. Well-being is defined by the Act as relating to a child's:

- physical and mental health and emotional well-being
- protection from harm and neglect
- education, training and recreation
- the contribution made by them to society
- social and economic well-being

Although most commonly used to refer to young people aged sixteen or under, 'children' in terms of the scope of this Act means those up to the age of eighteen.

**Children Act 1989**
For children and young people, the nature of the information that will be shared under this agreement may fall below a statutory threshold of s.47 (children in need of protection) or even s.17 (children in need of services). If the information to be shared does fall within these sections of the 1989 Act, then these will be the main legal gateway.

**Crime and Disorder Act 1998**
Section 115, provides a legal basis for sharing information with a relevant authority where the disclosure is necessary or expedient for the purposes of any provision of the Crime and Disorder Act 1998. Relevant authorities include: Police, Probation, Local Authorities, CCGs and certain NHS statutory bodies

**Human Rights Act 1998**
Gives force to the European Convention on Human Rights and, amongst other things, places an obligation on public authorities to protect people's right to life and right to be free from torture or degrading treatment".

There needs to be a balance between the desire to share, and a person's right to privacy under ***"The right to respect private and family life, home and correspondence".*** The local authority cannot interfere with this right except such as is necessary in the interests of national security, public safety or for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

**The Mental Capacity Act (MCA) 2005**.
Under the Mental capacity Act 2005 staff are required to apply 5 principles in their assessments to decide whether to share information without consent in a person's best interests.

The MCA Code of Practice, states: *it is important to balance people's right to make a decision with their right to safety and protection when they can't make decisions to protect themselves. The starting assumption must always be that an individual has the capacity, until there is proof that they do not.*

Under the Mental Capacity Act 2005 there would have to be good reasons for not undertaking an assessment of mental capacity regarding the decision to share information without consent, and these would need to be documented carefully.

**The Health and Social Care (health and adult social care services: information) Act 2012 and the seventh Caldicott principle:**
The Health and Social Care (health and adult social care services: information) Act 2012 has been amended by the Health and Social Care (Safety and Quality) Act 2015 by inserting a new requirement.

It places a new duty on commissioners or providers of health and adult social care to share information where this will facilitate care for an individual and

where it is in the individual's best interests, except where they have exercised their right to refuse consent. **This comes into force on 1st October 2015.**

This provides statutory support for the seventh Caldicott principle – "*the duty to share information can be as important as the duty to protect patient confidentiality*". The Act should be seen as providing a statutory basis for what is already recognised as good practice and a common law duty. It provides a more certain basis for interpretation of the Common Law Duty of Care and whenever it would be lawful and it would facilitate care in a person's best interests, then you must share relevant information.

However, it's also important to note that:

The new duty does not provide the authority to set aside Common Law Duty of Confidentiality requirements, nor does it remove the requirements of the Data Protection Act 1998. This means that where there is a duty of confidentiality or someone has made an informed decision to refuse consent to share data that must be respected except where an overriding consideration exists e.g. relating to the safety of another person or in relation to prevention or detection of crime.

The obligation to inform individuals about sharing (known as *fair processing*) continues to apply.

**Counter-Terrorism and Security Act 2015**

Section 26 of the Counter Terrorism and Security Act 2015 places a duty on *specified authorities* in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". Specified authorities include County and District/Borough Councils: Schools; Police; National Probation Service and Community Rehabilitation Companies; NHS Trusts and NHS Foundation Trusts;

The Prevent strategy has three specific strategic objectives:

- respond to the ideological challenge of terrorism and the threat we face from those who promote it;
- prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support; and
- work with sectors and institutions where there are risks of radicalisation that we need to address.

There is an expectation that authorities will work in partnership and share data where appropriate e.g. to ensure someone at risk of radicalisation is supported.

Information sharing must be assessed on a case-by-case basis and is governed by legislation. When considering sharing personal information, the specified authority should take account of the following:

- necessity and proportionality
- consent
- power to share;
- Data Protection Act
- Common Law Duty of Confidentiality.

Detailed guidance on Information Sharing in this context can be found in ***Prevent Duty Guidance:*** *Guidance for specified authorities in England and Wales on the duty in the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism*.

**Duty of Confidence**

Information held by agencies that will be shared as part of the Family Safeguarding Team's work is likely to have been gathered where a Duty of Confidence is owed.

A Duty of Confidence is not an absolute bar to disclosure, as information can be shared where there is a strong enough public interest to do so. It is the responsibility of the disclosing agency to ensure that the protection of children or other vulnerable persons would fulfil a public interest test before passing the information to a Partner.

When overriding the Duty of Confidence in the absence of consent, Partners must seek the views of the person representing the organisation that holds the Duty of Confidence and take these into account in relation to breaching the confidence. The originating Partner will be the final arbiter as to whether information is disclosed or not. The Partner may wish to seek specialist or legal advice if there is lack of clarity around justifiable disclosure of information. All disclosures must be relevant and proportionate to the intended aim of the disclosure and must be fully documented as an unjustified disclosure could lead to a claim for damages against the disclosing party.

**All staff** must be particularly mindful of their professional and ethical obligations and the public interest of confidence in the confidentiality of their services.

It may be necessary to seek advice on professional conduct as well as legal advice before sharing information without consent, especially for information related to the treatment of mental illness. All staff should ensure the need to protect children takes into account the children's rights as well as those of the adults concerned. Decisions will be reported to the Family Safeguarding Partnership Board for periodic review.

All information sharing decisions and the reason for that decision must be recorded at the time of the decision

**Appendix 1**

**First Principle: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—**
**(a) at least one of the conditions in Schedule 2 is met, and**
**(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met**

**Schedule 2** sets out the conditions necessary for any processing of personal data to take place. For the Family Safeguarding Project, the relevant principles are:
*1. The data subject has given his consent to the processing/sharing of information (implied consent may be acceptable)*
*2. The processing/sharing of information is necessary to meet any legal obligation to which the data*
*controller is subject*
*3. The processing is necessary in order to protect the vital interests of the data subject*
*4. The processing is necessary –*
*(b) for the exercise of any functions conferred on any person by or under any enactment*
*(d) for the exercise of any other functions of a public nature exercised in the public interest by any person*

*The processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject*

**Schedule 3** applies to sensitive data and a higher standard of consent is expected; ***it is likely that almost all of the data being shared through the Family Safeguarding Project will fall in to this category.***
In addition to the schedule 2 conditions, the following conditions of schedule 3 are likely to apply:
*1. The data subject has given explicit consent to the processing of the personal data.*
*2. The processing is necessary—*
*(a) in order to protect the vital interests (life or death) of the data subject or another person, in a case where: -*
*(i) consent cannot be given by or on behalf of the data subject, or.*
*(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or.*
*(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.*
*3. The processing—*
*(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),*
*(b) is necessary for the purpose of obtaining legal advice, or.*
*(c) is otherwise necessary for the purposes of establishing, exercising or*

*defending legal rights.*
*4, The processing is necessary—*
*(b) for the exercise of any functions conferred on any person by or under an enactment*
*5 The processing is necessary for medical purposes and is undertaken by—*
*(a) a health professional, or.*
*(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.*

**Second Principle: 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 or those purposes.**

- Information shared through this agreement is obtained solely for the purpose of promoting the safety and welfare of children and vulnerable adults and the prevention and detection of related crime.
- Information shared through this agreement will not be processed in any manner contradictory to that purpose.
- Each Partner is a Data Controller and responsible for issuing Privacy/Fair Processing Notices which accurately reflect this purpose and are accessible to all data subjects.
- Information explaining the Family Safeguarding Project and how it works is available on the council's website.

http://www.hertsdirect.org/your-council/hcc/childserv/aboutcs/futservchil/familysafeguarding/

**Third Principle: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed**

Due to the range of information systems in use among partner agencies for the Family Safeguarding Project, providing a definitive list of data fields to be shared is impractical. Once a referral has been received by the Family Safeguarding teams, decisions on which information systems will be scrutinised will be decided on a case by case basis. Only relevant and proportionate information will be shared where an organisation has a 'need-to-know' justification to see the information.

**Fourth Principle: Personal data shall be accurate and, where necessary, kept up to date**

The content and accuracy of shared information will be subject to each Partner's quality control procedures and validation

**Fifth Principle: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes**

Data destruction at the end of its retention period must be undertaken in accordance with organisational policies and Principle 7 of the Data Protection Act (see below).

**Sixth Principle: Personal data shall be processed in accordance with the rights of data subjects under this Act**

Partner agencies will respond to any notice from the Information Commissioner which imposes requirements to cease or change the way in which data is processed.

Each partner agency Data Controller is responsible for responding appropriately to Subject Access Requests addressed to them and to providing information to the data subject to enable them to make requests to other Partners where appropriate.

Data subjects have the right to object to processing. How the data subject makes such objections should be detailed in each partner's ***Privacy Notice***.

Data subjects have the right to correct inaccuracies in their record. Each Partner must have policies and processes in order to comply with DPA Principle 4. These should be employed in the event of such a notification and, where it relates to data obtained through a Partner, the originating Partner should be notified.

Information about how people can gain access to information HCC hold about them is published on the Herts Direct website at:

http://www.hertsdirect.org/your-council/work/foi/whtpersdt/

**Seventh Principle: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data**

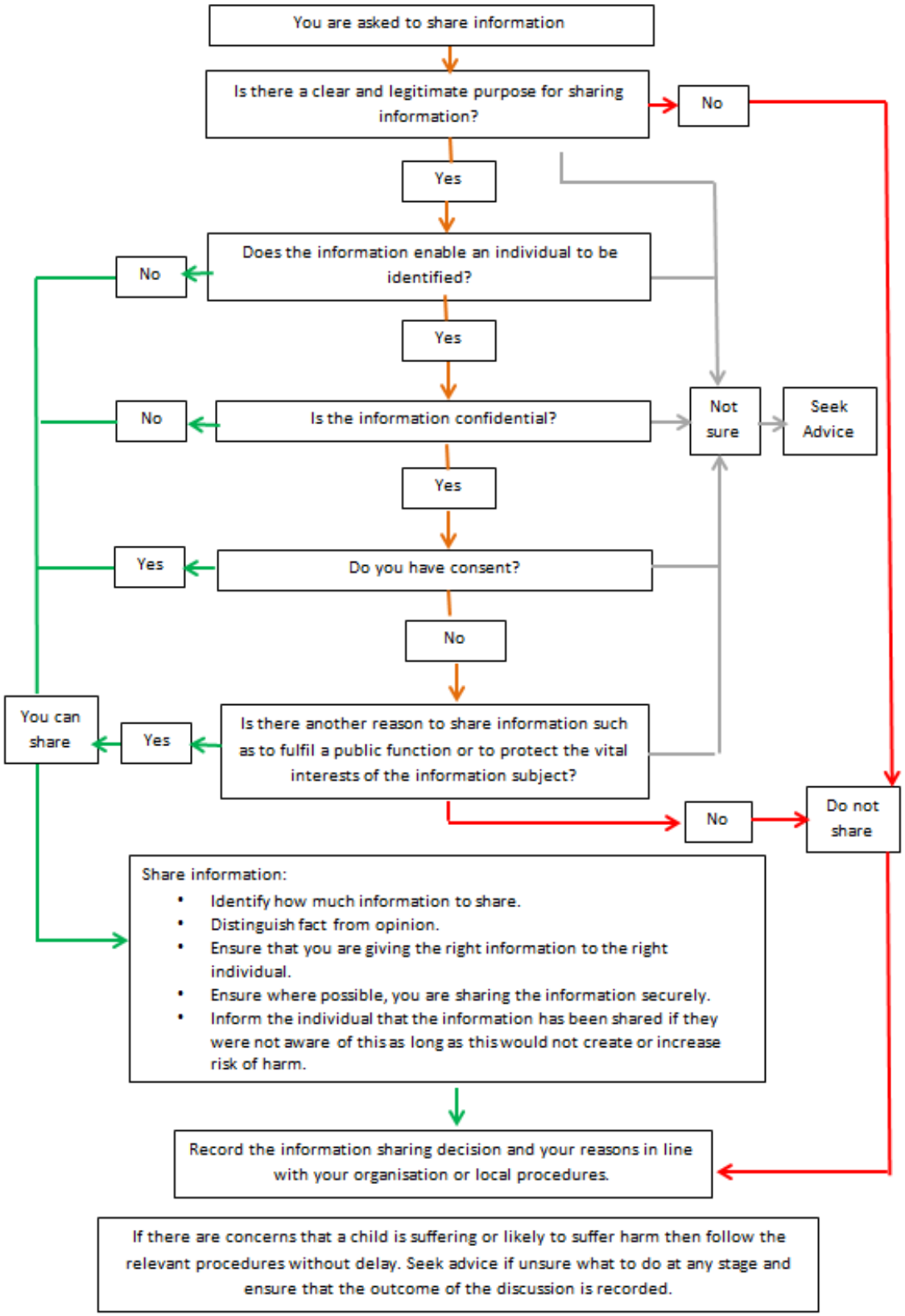
Partner agencies are responsible for the technical and organisational, physical and technical security measures to satisfy the Seventh Principle in respect of their own systems and staff.
Personal Data will only be transferred between agencies by Secure email or HertsFX.

**Eighth Principle: 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**

Under the terms of this agreement no information will be passed outside of the European Economic Area unless specific requirement exists and the originating organisation makes that decision for a particular reason in relation to the safeguarding of a child, young person or adult with a safeguarding need. Legal advice may be necessary in these cases.

Where any information systems are hosted externally to the partner organisations, data must be stored within countries of the European Economic Area.

**Appendix 2**


You are asked to share information
Is there a clear and legitimate purpose for sharing information?
No
Yes
Does the information enable an individual to be identified?
No
Yes
Is the information confidential?
No
Not sure
Seek Advice
Yes
Do you have consent?
Yes
No
Is there another reason to share information such as to fulfil a public function or to protect the vital interests of the information subject?
Yes
You can share
No
Do not share
Share information:
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, you are sharing the information securely.
Inform the individual that the information has been shared if they were not aware of this as long as this would not create or increase risk of harm.
Record the information sharing decision and your reasons in line with your organisation or local procedures.
If there are concerns that a child is suffering or likely to suffer harm then follow the relevant procedures without delay. Seek advice if unsure what to do at any stage and ensure that the outcome of the discussion is recorded.