Derbyshire Partnership Forum

Information Sharing Protocol

Document owner	Derbyshire Partnership Forum
Document author and enquiry point	Hannah Edwards, Information Development Manager, Derbyshire Community Health Services NHS Trust Hannah.edwards@nhs.net
Review date of document	
Version	3.3
Changes made since last version	o Flowchart of key questions for information sharing added as appendix 4. o Consent section expanded to include children's consent and mental capacity act o Small amendments to update content o Reference to pseudonymisation added o 5.2 added on Caldicott Principles o 8.7 expanded with examples of disclosure without consent. o 11.3 added. o Appendix 5 – Case Studies – added. o Section on flowchart explanations (in appendix 4) added. o Appendix 6 added to include signatories list. o EEA definition updated in Appendix 2
Document classification	**DRAFT**
Next document review date	

Table of Contents

1. Introduction

1.1 The Derbyshire Partnership Forum is committed to working together for the delivery of improved public services to the people of Derbyshire. It is recognised that the lawful sharing of information between partner agencies is essential to meet these aims.

1.2 The Derbyshire Partnership Forum Information Sharing Protocol has been established to help support these aims.

1.3 This document is an Information Sharing Protocol for key organisations in Derbyshire. Its aim is to facilitate sharing of information between the public, private and voluntary sectors so that the public receive the services they need.

1.4 Organisations involved in providing services to the public have a legal responsibility to make sure that their use of personal information is lawful, properly controlled and that an individual's rights are respected.

2. Scope

2.1 This top level Protocol sets out the principles for information sharing between partner organisations. See Derbyshire Partnership Forum Website for membership details.

2.2 This Protocol sets out the minimum rules that all people working for or with the partner organisations must follow when using and sharing information.

2.3 The Protocol applies to the following information:

- all personal information processed by the organisations including electronically such as computer systems, CCTV, audio or in manual records
- aggregated and anonymised data
- commercial or business, sensitive data

2.4 This Protocol may be extended further to include other public sector, private and voluntary organisations working in partnership to deliver services.

3. Aims and objectives

3.1 The aim of this Protocol is to provide a framework for the partner organisations to establish and regulate working practice. The Protocol also provides guidance to make sure information is securely transferred and that information is shared for justifiable 'need to know' purposes.

3.2 These aims intend to:

- guide partner organisations on how to share personal information lawfully
- explain the security and confidentiality laws and principles of information sharing
- increase awareness and understanding of the key issues
- emphasise the need to develop and use information sharing agreements
- support a process, which will monitor and review all data flows
- encourage a two-way flow of data where applicable

- protect the partner organisations from accusations of wrongful use of sensitive personal information
- identify the lawful basis for information sharing

3.3 By becoming a partner to this Protocol, partner organisations are making a commitment to:

- follow and apply HM Government's 'Information Sharing: Guidance for practitioners and managers' (see appendix 4 for the flowchart of key questions for information sharing) available at: https://www.education.gov.uk/publications/standard/Integratedworking/Page1/DCSF-00807-2008
- apply the Information Commissioner's Code of Practice's 'Fair Processing' and 'Best Practices' Standards
- comply with the Data Protection Act 1998
- develop local information sharing agreements that specify transaction details. See appendix 3 for template.

3.4 All partners are expected to train relevant staff and promote awareness of the major requirements of information sharing, including responsibilities in confidentiality and data protection. Appropriate policies and procedures will be produced where required to support this and be made available to all employees through the partners' Intranet sites and through other communication methods.

4. The legal framework

4.1 The principal legislation concerning the protection and use of personal information is listed below, further explained in Appendix 1.

- Human Rights Act 1998 - Article 8
- The Freedom of Information Act 2000
- Data Protection Act 1998
- The Common Law Duty of Confidence

4.2 Other legislation and/or standards may be relevant when sharing specific information. For example, Children Acts 1989, 2004; Crime and Disorder Act 1998; The Education Act 1996; Health Act 1999; Health and Social Care Act 2001; Mental Health (Patients in the Community) Act 1995; National Health Service and Community Care Act 1990; The Regulation of Investigatory Powers Act 2000.The Caldicott Principles; The NHS Information Governance Framework; The Government Protective Marking Scheme, Mental Health Capacity Act.

5. Data covered by this protocol

5.1 This protocol applies to all personal, anonymised and pseudonymised information as defined in the Data Protection Act 1998 (DPA). Anonymised or pseudonymised data should be used wherever possible.

5.2 The Caldicott Principles must be followed whenever patient information or data is being transferred.

5.3 Personal Information

5.3.1 The term 'personal information' refers to **any** information held as either manual or electronic records, or records held by means of audio and/or visual technology, about an individual who can be personally identified from that information.

5.3.2 The term is further defined in the DPA as:
data relating to a living individual who can be identified from those data, or any other information which is in the possession of, or is likely to come into the possession of, the data controller – the person or organisation collecting that information.

5.3.3 The DPA also defines certain classes of personal information as '**sensitive data**' where additional conditions must be met for that information to be used and disclosed lawfully. "Sensitive personal data" relates to the racial or ethnic origin of a data subject, their political opinions, religious beliefs, trade union membership, sexual life, physical or mental health or condition or criminal offences or record.

5.3.4 An individual may consider certain information about themselves to be particularly 'sensitive' and may request other data items to be kept especially confidential.

5.3.5 In certain circumstances, although not all, people have a legal right to choose how their data is used and who may have access to it. As far as possible, depending on the circumstances under which the data is collected, their individual wishes should be respected. **Any** personal information about an individual should be treated as sensitive.

5.4 Anonymised data

5.4.1 Make sure that anonymised information does not identify an individual, either directly or by summation.

5.4.2 Data about an individual can be shared without their consent in a form where the identity of the individual cannot be recognised. For example when:
- reference to any data item that could lead to an individual being identified has been removed
- the data cannot be combined with any other data sources held by a partner to produce personal identifiable data.

5.4.3 Anonymising data does not remove the duty of confidence.

5.5 Pseudonymised data

5.5.1 Pseudonymising involves the removing of identifiers from patient, client and staff data so that those using the data cannot identify them. The use of a pseudonym means that, where approved and appropriate, it is possible to link the data back to the source (and identifiable) data if required.

6. Purposes for sharing information

6.1 Information should only be shared for a specific lawful purpose or when appropriate consent has been obtained. See appendix 4 for a flowchart of the key questions for information sharing.

6.2 Employees should only have access to personal information on a justifiable **need to know** basis, in order for them to perform their duties in connection with the care they are there to deliver.

6.3 Having this agreement does not give license for unrestricted access to information another partner organisations may hold. It lays the parameters for the safe and secure sharing of information for a justified **need to know** purpose.

6.4 All employees have an obligation to protect confidentiality and a duty to ensure that information is only disclosed to those who have a right to see it.

6.5 All employees should be trained and be fully aware of their responsibilities to maintain the security and confidentiality of personal information.

6.6 All staff should follow the procedures and standards that have been agreed and incorporated within this Information Sharing Protocol and any associated information sharing agreements.

6.7 Each partner organisation will operate lawfully in accordance with the eight Data Protection Principles, see Appendix 1.

6.8 Personal data shall not be transferred to a country or territory outside the European Economic Area without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

7. Restrictions on use of shared information

7.1 Information must only be used for the purpose(s) specified at the time of disclosure(s). It is a condition of access that it must not be used for any other purpose without the permission of the Data Controller who supplied the data, unless an exemption applies within the Data Protection Act 1998.

7.2 Additional statutory restrictions apply to the disclosure of certain information. For example criminal records, HIV and AIDS, assisted conception and abortion, child protection.

7.3 It is recognised that Partners' organisational policies and procedures may place additional restrictions on the sharing of information. For example, limitations on the electronic transfer of information where secure communications cannot be guaranteed.

8. Consent

8.1 Everyone aged 16 or over is presumed to be competent and have mental capacity to give informed consent for themselves unless the opposite is demonstrated. Children between the ages of 12 and 16 who have the capacity and understanding to make decisions about their own treatment are also entitled to decide whether personal information may be passed on and to have their confidence respected. If a child is not able to demonstrate competence to consent, someone with parental responsibility may do so on their behalf.

8.2 Anyone with Lasting Power of Attorney (LPA), for health and welfare or property and affairs, for the patient under the Mental Capacity Act, may have been donated the power to make decisions on the person's behalf. The same information that would have been shared with the person to make an informed decision would be shared with the LPA. Refer to the Mental Capacity Act and Code of Practice for further specific guidance.

8.3 Where a partner organisation has a statutory obligation to disclose personal information, then the consent of the data subject is not required. However, the data subject should be informed that such an obligation exists.

8.4 If a partner organisation decides not to disclose some or all of the personal information, the requesting authority must be informed. For example, the partner organisation may be relying on an exemption or on the inability to obtain consent from the data subject.

8.5 Consent has to be signified by some communication between the organisation and the data subject. If the data subject does not respond this cannot be assumed as implied consent.

8.6 If consent is used as a form of justification for disclosure, the data subject must have the right to withdraw consent at any time. When using sensitive data, explicit consent must be obtained. In such cases, the data subject's consent must be clear. It must cover items such as the specific details of processing, the data to be processed and the purpose for processing.

8.7 Consent is not the only means by which data can be disclosed. Under the Data Protection Act 1998, to disclose personal information at least one condition in schedule 2 must be met. To disclose sensitive personal information, at least one condition in both schedules 2 and 3 must be met. Appendices 1 and 2 contain more information. Examples of where information may be disclosed without consent are for the prevention, detection or prosecution of serious crime, or where a child or adult is believed to be at risk of harm.

9. Organisational responsibilities

9.1 Each partner organisation is responsible for making sure that their organisational and security measures protect the lawful use, confidentiality, integrity and availability of information shared under this Protocol.

9.2 Partner organisations will accept the security classifications on information and handle the information accordingly.

9.3 Partner organisations accept responsibility for jointly auditing compliance with the information sharing agreements in which they are involved.

9.4 Partner organisations should make it a condition of employment that its employees will abide by its rules and policies on the protection and use of confidential information. This condition should be written into employment contracts and any failure by an employee to follow the policy should be dealt with in accordance with that organisation's disciplinary procedures.

9.5 Partner organisations should make sure that their contracts with external service providers abide by their rules and policies on the protection and use of confidential information.

9.6 The partner organisation originally supplying the information should be notified of any breach of confidentiality, or incident, involving a risk or breach of the security of information.

9.7 Partner organisations should have documented policies for records retention, maintenance and secure waste destruction.

10. Individual responsibilities

10.1 Every employee working for the organisations listed in this Partnership Agreement:

- is personally responsible for the safekeeping of sensitive information they obtain, handle, use and disclose
- should know how to obtain, use and share information they legitimately need to do their job
- has an obligation to request proof of identity, or take steps to validate the authorisation of another before disclosing sensitive information
- must uphold the general principles of confidentiality, follow the rules laid down in this Protocol and seek advice when necessary
- should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal
- should ensure any information is transferred using an approved, secure method of transportation in accordance with their organisation's policies and procedures

10.2 Every employee working for the organisations listed in this Agreement must ensure they follow their own organisation's policies and procedures before releasing any information under this agreement.

11. General principles

11.1 The principles outlined in this protocol are recommended good standards of practice or legal requirements that should be followed equally across all services.

11.2 This protocol sets the core standards applicable to all partner organisations and should be the basis of all information sharing agreements established to secure the flow of personal information.

11.3 This protocol has been developed to enable appropriate and effective information sharing and is not intended to be a 'barrier' to sharing.

11.4 This protocol should be used together with local service level agreements, contracts or any other formal agreements that exist between the partner organisations.

11.5 All parties signed up to this protocol are responsible for making sure that they have organisational measures to protect the security and integrity of personal information and that their employees are properly trained to understand their responsibilities and comply with the law.

11.6 This protocol has clear and consistent principles that satisfy the requirements of the law that all employees must follow when using and sharing personal information.

11.7 The specific purpose for using and sharing information will be defined in the information sharing agreements that will be specific to the partner organisations sharing information.

12. Review arrangements

12.1 The Derbyshire Partnership Forum will ensure this Protocol is formally reviewed bi-annually, unless new or revised legislation or national guidance necessitates an earlier review.

12.2 Any of the signatories can request an extraordinary review at any time when a joint discussion or decision is necessary to tackle local service developments.

Appendix 1 - Relevant Legislation

Data Protection Act 1998

The **Data Protection Act 1998** governs the protection and use of **personal** information - data that relates to a living individual who can be identified. The Act does not apply to personal information about people who have died.

Any organisation processing, obtaining, holding, using, disclosing and disposing of data is a 'Data Controller' responsible for abiding by the eight data protection principles and notifying the Information Commissioner of that processing.

The Act gives seven rights to individuals about their own personal data:

- Right of subject access
- Right to prevent processing likely to cause damage or distress
- Right to prevent processing for the purposes of direct marketing
- Rights in relation to automated decision taking
- Right to take action for compensation if the individual suffers damage or damage and distress, as a result of any breach of the act.
- Right to take action to rectify, block, erase or destroy inaccurate data
- Right to request the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

The eight key principles of the Act are:

1. Personal data shall be processed fairly and lawfully and shall not be processed unless at least one of the conditions in Schedule 2 is met and for 'sensitive personal data' at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained for specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose/purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose/purposes for which they are processed.
4. Personal data shall be accurate and, where necessary kept up-to-date
5. Personal data shall not be kept for longer than is necessary for that purpose/purposes.
6. Personal data shall be processed in accordance with the rights of the data subject under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, EEA, without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

Seventh Principle – Interpretation

The Act gives some further guidance on issues that should be considered in deciding whether security measures are 'appropriate'. These are:

- taking into account the state of technological development at any time and the costs of implementing any measures. The measures must ensure a level of security appropriate to:-
  - the harm that might arise from a breach of security; and
  - the type of data to be protected.

- The data controller must take reasonable steps to ensure the reliability of employees having access to the personal data.

Some of the security controls that the data controller is likely to need to consider include:

- security management
- controlling access to information
- ensuring business continuity
- employee selection and training
- detecting and dealing with breaches of security.

The Act has express obligations on data controllers when processing of personal data is done by a data processor on behalf of the data controller. To comply with the seventh principle the data controller must:

- choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures they take;
- take reasonable steps to ensure compliance with those measures; and
- make sure that the processing by the data processor is done under a contract, which is made or evidenced in writing, under which the data processor is to act only on instructions from the data controller. The contract must require the data processor to comply with obligations equivalent to those imposed on the data controller by the seventh principle.

Further advice is in BS 7799 and ISO/IEC Standard 17799.

It is important to note that the seventh principle relates to the security of the processing as a whole and the measures to be taken by data controllers to provide security against any breaches of the Act rather than just breaches of security.

Schedule 2 and Schedule 3 conditions

Conditions for processing personal data are that one condition in Schedule 2 should be met.

Conditions for processing sensitive personal data are that one condition in Schedule 2 and a condition in Schedule 3 should also be met.

Schedule 2: Personal data Schedule 3: Sensitive personal data

The data subject has given consent, or the processing is necessary for:-

- a contract
- a legal obligation
- protection of the vital interests
- public function
- in the public interest
- a statutory obligation
- legitimate interests of the data controller.

The data subject has given explicit consent, or the processing is necessary for:-

- employment-related purposes
- the purpose of, or in connection with, legal proceedings
- protect the vital interests of the individual when consent cannot be obtained
- made public by the data subject
- a substantial public interest
- preventing or detecting an unlawful act
- the legitimate interests of a non-profit data controller making organisation
- medical purposes by a health professional.

The Human Rights Act 1998

The Human Rights Act 1998 incorporates into our domestic law certain articles of the European Convention on Human Rights, ECHR. The Act requires all domestic law to be read compatibly with the Convention Articles.

It also places a legal obligation on all public organisations to act in a manner compatible with the Convention. If a public organisation fails to do this, then it may be the subject of a legal action under section 7. This is an obligation not to violate convention rights, but a positive obligation to uphold these rights.

Sharing of information between agencies has the potential to infringe a number of convention rights. In particular, Article 3 - Freedom from torture or inhuman or degrading treatment, Article 8 - Right to respect for private and family life and Article 1 of Protocol 1 - Protection of Property.

The qualification of Article 8 is ‘there shall be no interference by a public organisation with this right unless it is in the interests of national security, public safety, the economic well being of the country, the prevention of disorder and crime, the protection of health and morals, or the protection of the rights and freedoms of others’.

In addition, all convention rights must be secured without discrimination on a wide variety of grounds under article 14.

The convention does allow interference with the convention rights by public organisations, under certain broadly defined circumstances known as legitimate aims. However, mere reliance on a legal power may not alone provide sufficient justification and they must consider these:

- Is there a legal basis for the action being taken?
- Does it pursue a legitimate aim as outlined in the particular Convention Article?
- Is the action taken proportionate and the least intrusive method of achieving that aim?

Article 8.1 provides that ‘everyone has the right to respect for his private and family life, his home and his correspondence.’

Article 8.2 provides ‘there shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country for the prevention of crime and disorder, for the protection of health and morals or for the protection of the rights and freedoms of others.’

Other legislation, guidance and standards

Other Acts apply to further specify these exceptions. For example **Prevention of Terrorism Act 2002, Health and Social Care Act 2000, Regulation of Investigatory Powers Act RIPA2000.** Further information about these or any other relevant legislation is on the HMSO website http://www.hmso.gov.uk

The Freedom of Information Act - 2000

The Freedom of Information Act 2000 applies to all public organisations and started coming into force in 2003.

The Act creates new rights of access to information - rights of access to personal information will remain under the Data Protection Act - and revises and strengthens the Public Records Act 1958 and 1967 by re-enforcing records management standards of practice.

The Lord Chancellor has issued a code of practice on the management of records under Freedom of Information. The principle is that *'any freedom of information legislation is only as good as the quality of the records to which it provides access. Such rights are of little use if reliable records are not created in the first place'.* Further information guidance is on the following web site www.informationcommissioner.gov.uk.

The Common Law Duty of Confidence

The Common Law Duty of Confidence requires that information that has been provided in confidence may only be used for purposes of which the subject has been informed and given their consent unless a specific statutory requirement exists.

The duty is not absolute but may only be overridden if the holder of the information can justify disclosure as being in the public interest for example to protect others from harm.

Caldicott Principles

When sharing person-identifiable information, the Caldicott principles should be applied:

- Justify the purpose – why is the information required
- Don't use patient-identifiable information unless it is absolutely necessary
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information is on a strict need-to-know basis
- Everyone with access to patient-identifiable information should be aware of his or her responsibilities
- Understand and comply with the law

Appendix 2 - Glossary of terms

Accessible record – unstructured personal information, usually in manual form relating to health, education, social work and housing.

Agent – acts on behalf of the data subject.

Aggregated – collated information in table format.

Anonymous data – If the Data Controller has information that allows data subjects to be identified, the Information Commissioner would rule it is **not** anonymous data. This is regardless of whether or not they intend to identify individuals. The Data Controller must be able to justify why and how the data is no longer personal.

CCTV – close circuit television.

Consent – to give permission or approval for something to happen.

Consent – the Information Commissioner's legal guidance to the Data Protection Act 1998 is to refer to the Directive, which defines consent as '…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed' (3.1.5).

Data is information:-

- being processed by means of equipment operating automatically or
- recorded with the intention it will be processed by such equipment or
- recorded as part of a relevant filing system or
- the three items listed forming part of an accessible record but not part of it.

Data Controller – a person or a legitimate organisation such as a business or public authority who jointly or alone determines the purposes for which personal data is processed.

Data flows – the movement of information internally and externally, both within and between organisations.

Data Processing – any operation performed on data. The main examples are collecting, retaining, deleting, using and disclosing data.

Data Processor – operates on behalf of the Data Controller. Not the organisations employees.

Data set – a defined group of information.

Data Subject – an individual who is the subject of personal information.

Disclosure –passing information from the Data Controller to another organisation or an individual.

Duty of confidence – everyone has a duty under common law to safeguard personal information.

EEA – this consists of the twenty-seven European Union members together with Iceland, Liechtenstein and Norway.

Fair processing – to inform the Data Subject how the data is to be processed before processing starts.

Health professional – In the Data Protection Act 1998, 'health professional' means any of the following who is registered as:-

- a medical practitioner, dentist, optician, pharmaceutical chemist, nurse, midwife or health visitor, and osteopaths.

and

- any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 currently extends. Clinical psychologists, child psychotherapists and speech therapist, music therapists employed by a health service body, and scientists employed by an organisation as head of department.

Health record – any information relating to health, produced by a health professional.

Need to know – to supply the minimum amount of information required for the defined purpose.

Personal data – means data relating to a living individual who can be identified from those data, including opinion and expression of intention.

Purpose – the use or reason for which information is stored or processed.

Recipient – anyone who receives personal information except statutory bodies for the purpose of specific inquiries.

Relevant filing system – two levels of structure:

- filing system structured by some criteria
- each file structured so that particular information is readily accessible.

Sensitive personal data – data concerning racial origin, politics, trade union activity, health, sexuality, offending and so on.

Serious crime – There is no absolute definition of 'serious' crime, but section 116 of the Police and Criminal Evidence Act 1984 identifies some 'serious arrestable offences'. These include:-

- treason
- murder
- manslaughter
- rape
- kidnapping
- certain sexual offences
- causing an explosion
- certain firearms offences
- taking of hostages
- hijacking
- causing death by reckless driving
- offences under Prevention of Terrorism legislation - disclosures nowcovered by the Prevention of Terrorism Act 1989.

Subject access – the individual's right to obtain a copy of information held about themselves.

Third party – any person who is not the data subject, the data controller, the data processor. This includes health, housing, education, carers, voluntary sector workers as well as members of the public.

Appendix 3 - Information Sharing Agreements guidance notes

Include any necessary sections:

1. **List of Partners to the agreement**

Who are the intended Partners to this Agreement and what are their responsibilities?

2. **Information to be shared**

What is the specific business need/objective for information sharing?

3. **Purpose of information sharing**

What specific information is required for the purpose of this agreement?
Include an explanation of how anonymised information may be used where appropriate.

4. **Basis for information sharing**

What are the specific lawful powers/obligations for the processing of information? And, What considerations apply to make the processing fair under the terms of the Data Protection Act 1998? Please also state which conditions of Schedule 2 and Schedule 3 are relevant to this sharing.

5. **Exchange of information**

State explicity how and what information is to be shared, consider methods such as encrypted email, mail, fax and how regularly these are to take place.

6. **Terms of use of the information**

Add a clear statement of how the information is intended to be used and any restrictions which may apply.

7. **Data quality assurance**

Explain what standards will apply for data quality and how errors will be handled.

8. **Data Retention, Review and Disposal**

Explain how long the information is intended to be retained for the purpose and any specific review or disposal arrangements that apply.

9. **Access and Security**

Explain the standards and conditions which are required to protect the information concerned. Include any special arrangements which might apply. For example access to files will be restricted – operate a clear desk policy, employees given access on a need to know basis.

10. **General Operational Guidance**

Include or reference any general operational guidance which is relevant to the purpose of the agreement that is not covered in any other section. Details of relevant contacts can be appended to the document.

11. **Management of the Agreement**

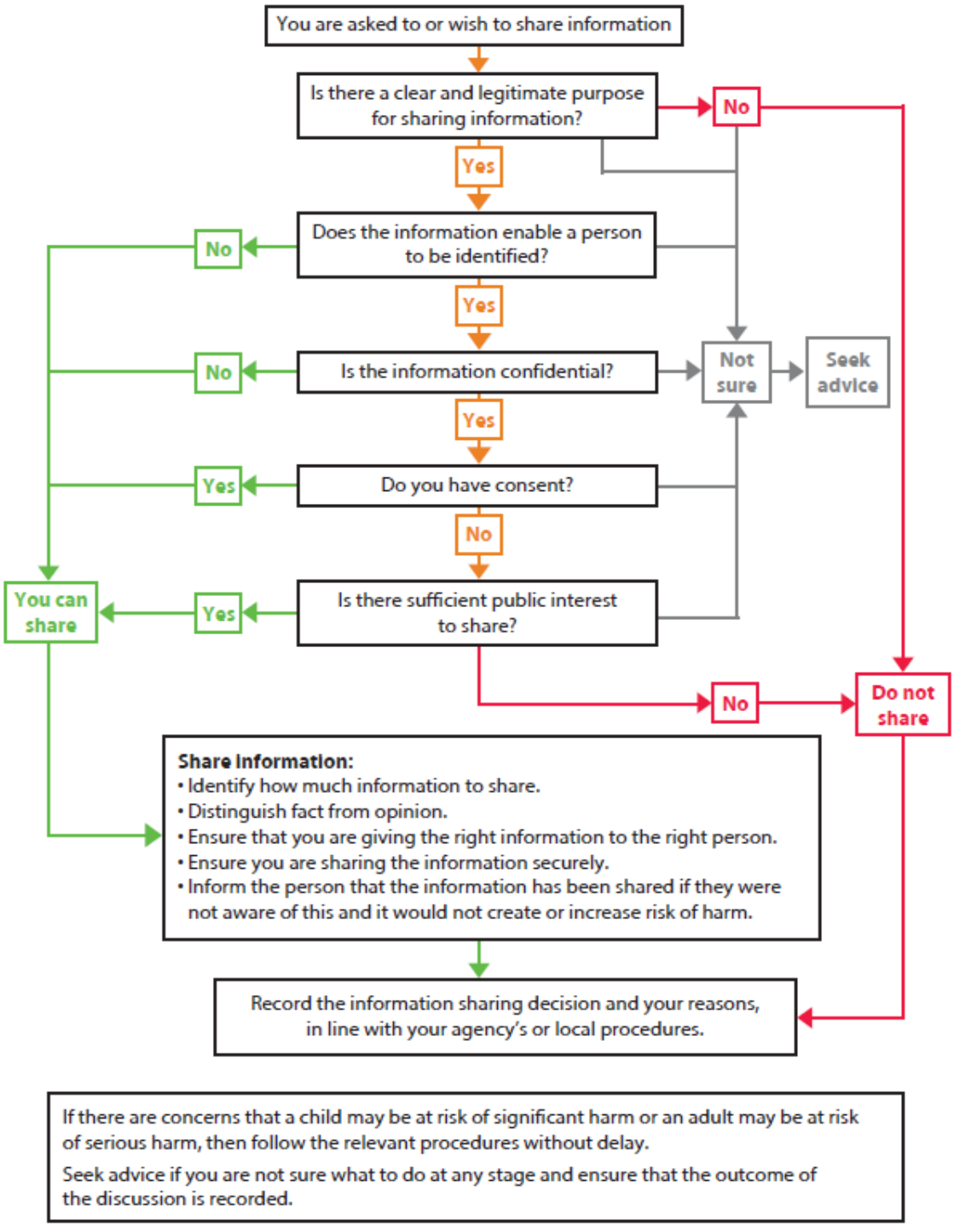
Additional information should be provided to address:-

- Handling of complaints or breaches of the agreement
- Handling of requests for information under Data Protection/Freedom of Information
- Appropriate Signatories
- Review of the Agreement
- Compliance with the Agreement
- Closure/termination of agreement
- Indemnity

Appendix 4 - Flowchart of key questions for information sharing

Source: HM Government 'Information Sharing: Guidance for practitioners and managers https://www.education.gov.uk/publications/standard/Integratedworking/Page1/DCSF-00807-2008

See the next page for further detail on some of the sections in the flowchart.



Explanation of some of the flowchart sections:

These explanations are taken from HM Government 'Information Sharing: Guidance for practitioners and managers. The full explanations have not been included in this document and so please also refer to the full Guidance, available at: https://www.education.gov.uk/publications/standard/Integratedworking/Page1/DCSF-00807-2008

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

Whether you work for a statutory or non-statutory service, any sharing of information must comply with the law relating to confidentiality, data protection and human rights. Establishing a legitimate purpose for sharing information is an important part of meeting those requirements.

- **Does the information enable a living person to be identified?**

If the information is anonymised, it can be shared. However, if the information is about an identifiable individual or could enable a living person to be identified when considered with other information, it is personal information and is subject to data protection and other laws.

- **Is the information confidential?**

Confidential information is:
• personal information of a private or sensitive5 nature; and
• information that is not already lawfully in the public domain or readily available from another public source; and
• information that has been shared in circumstances where the person giving the information could reasonably expect that it would not be shared with others.

This is a complex area and you should seek advice if you are unsure.

- **Do you have consent to share?**

Consent issues can be complex and a lack of clarity about them can sometimes lead practitioners to assume incorrectly that no information can be shared. Page 17 of the Gudance document gives further information to help you understand and address the issues.
It covers:
• what constitutes consent;
• whose consent should be sought; and
• when consent should not be sought.

- **Is there sufficient public interest to share the information?**

Even where you do not have consent to share confidential information, you may lawfully share it if this can be justified in the public interest. Seeking consent should be the first option. However, where consent cannot be obtained or is refused, or where seeking it is inappropriate or unsafe, the question of whether there is a sufficient public interest must be judged by the practitioner on the facts of each case. **Therefore, where you have a concern about a person, you should not regard refusal of consent as necessarily precluding the sharing of confidential information.**

A public interest can arise in a wide range of circumstances, for example, to protect children from significant harm, protect adults from serious harm, promote the welfare of children or prevent crime and disorder. There are also public interests, which in some circumstances may weigh against sharing, including the public interest in maintaining public confidence in the confidentiality of certain services.

- **Are you sharing information appropriately and securely?**

If you decide to share information, you should share it in a proper and timely way, act in accordance with the principles of the Data Protection Act 1998, and follow your organisation's policy and procedures.

- **Have you properly recorded your information sharing decision?**

You should record your decision and the reasons for it, whether or not you decide to share information. If the decision is to share, you should record what information was shared and with whom.

Appendix 5 – Case Studies

These are taken from Information Commissioner's Office "Data Sharing Code of Practice" available at:
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/data_sharing.aspx

1. A local university wants to conduct research into the academic performance of children from deprived family backgrounds in the local area. The university wants to identify the relevant children by finding out which ones are eligible for free school meals. Therefore, it wants to ask all local primary and secondary schools for this personal data, as well as the relevant children's test results for the past three years.
    - The DPA contains various provisions that are intended to facilitate the processing of personal data for research purposes. However, there is no exemption from the general duty to process the data fairly. Data about families' income levels, or eligibility for benefit, can be inferred fairly reliably from a child's receipt of free school meals. Parents and their children may well object to the disclosure of this data because they consider it sensitive and potentially stigmatising. Data about a child's academic performance could be considered equally sensitive.
    - The school could identify eligible children on the researchers' behalf and contact their parents, explaining what the research is about, what data the researchers want and seeking their consent for the sharing of the data.
    - Alternatively, the school could disclose an anonymised data set, or statistical information, to the researchers.
    - There is an exemption from subject access for data processed only for research purposes, provided certain conditions are satisfied, for example the research results are not made available in a form which identifies anyone. However, it is good practice to provide data subjects with access to their personal data wherever possible. If subject access is going to be refused, for example because giving access would prejudice the research results, this should be explained to individuals during the research enrolment process.

2. A group of police forces are cooperating with immigration officials to collect evidence about a number of individuals thought to be involved in people trafficking. This involves exchanging data about suspects' whereabouts and activities.
    - There is no need to tell any of the suspects that personal data about them is being collected or exchanged. This is because doing so would 'tip off' the suspects, allowing them to destroy evidence, prejudicing the likelihood of prosecution.
    - The police, or immigration agency, may still need to provide subject access to the data, and explain their collection and sharing of the data, when doing so will no longer prejudice the prosecution.

3. Two neighbouring health authorities want to share information about their employees because they have been informed that certain individuals are apparently being employed by both health authorities and are working the same shift pattern at each.
    - The health authorities involved should make it clear to their staff that they are carrying out an anti-fraud operation of this sort. They should explain what data will be shared, who it will be shared with and why it is being shared.
    - If possible, the health authorities should only share data about particular employees who are suspected of fraudulent behaviour.

- However, if data about all employees is to be matched, any discrepancies should be recorded and investigated, and data about all the other employees should be deleted or returned to the original health authority.

4. A council is outsourcing work previously carried out by its children and family services department to a charity. The charity will need details of the families currently receiving services to take over the council's role. The council writes to customers to tell them what is happening. As customers have no option but to deal with the new provider if they want to continue to receive their services, the council's letter should explain clearly who will be providing the service and what information will be passed over. It should reassure customers that information will continue to be used for the same purposes.

5. A local authority is required by law to participate in a nationwide anti-fraud exercise that involves disclosing personal data about its employees to an anti–fraud body. The exercise is intended to detect local authority employees who are illegally claiming benefits that they are not entitled to.
   - Even though the sharing is required by law, the local authority should still inform any employees affected that data about them is going to be shared and should explain why this is taking place unless this would prejudice proceedings.
   - The local authority should say what data items are going to be shared – names, addresses and National Insurance numbers – and provide the identity of the organisation they will be shared with.
   - There is no point in the local authority seeking employees' consent for the sharing because the law says the sharing can take place without consent. The local authority should also be clear with its employees that even if they object to the sharing, it will still take place.
   - The local authority should be prepared to investigate complaints from employees who believe they have been treated unfairly because, for example, their records have been mixed up with those of an employee with the same name.

Appendix 6 – List of Signatories to this Protocol

Organisations signed up to this protocol are:
SIGNATURES of Chief Executives of all Partner organisations

Chesterfield Royal Hospital NHS Foundation Trust Signature:…….. Date: …….. Chief Executive Name: …….
Derby City Council Signature:…….. Date: …….. Chief Executive Name: …….
Derby Hospitals NHS Foundation Trust Signature:…….. Date: …….. Chief Executive Name: …….
Derbyshire Healthcare NHS Foundation Trust Signature:…….. Date: …….. Chief Executive Name: …….
Derbyshire Community Health Services NHS Trust Signature:…….. Date: …….. Chief Executive Name: …….
Derbyshire and Nottingham Local Area Team Signature:…….. Date: …….. Chief Executive Name: …….

Derbyshire Health United Signature:…….. Date: …….. Chief Executive Name: …….
Derbyshire County Council Signature:…….. Date: …….. Chief Executive Name: …….
East Midlands Ambulance Service Signature:…….. Date: …….. Chief Executive Name: …….
Erewash Clinical Commissioning Group Signature:…….. Date: …….. Chief Executive Name: …….
Hardwick Clinical Commissioning Group Signature:…….. Date: …….. Chief Executive Name: …….
North Derbyshire Clinical Commissioning Group Signature:…….. Date: …….. Chief Executive Name: …….
Southern Derbyshire Clinical Commissioning Group Signature:…….. Date: …….. Chief Executive Name: …….