

Contents

	Page No
1. Introduction	3
2. Scope	4
3. Aims and Objectives	5
4. The Legal Framework	6
5. Information Covered by this Protocol	7
6. Purposes for Sharing Information	8
7. Restrictions on the Use of Information Shared	9
8. Consent	10
9. Organisational Responsibilities	11
10. Individual Responsibilities	12
11. General Principles	13
12. Review Arrangements	14
Appendix 1: Signatures and Contact Information	15
Appendix 2: Relevant Legislation	16 - 21
Appendix 3: Glossary of Terms	22 - 24
Appendix 4: Information Sharing Agreement Template	25 - 28

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 and has developed this high level Information Sharing Protocol.
- 1.3 The Derbyshire Partnership Forum and Derbyshire Information Access Group have endorsed this document.
- 1.4 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.
- 1.5 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. This balance between the need to share information to provide quality service and to protect confidentiality is often a difficult one.
- 1.6 The legal situation on the protection and use of personal information can be unclear. This may lead to information not being readily available to those who have a genuine need to know so that they can do their job properly. See Appendix 2 for relevant legislation.
- 1.7 This document will supersede the Crime and Disorder Partnerships Joint Protocol on Information Exchange agreed in 2000. Other existing information sharing agreements will be reviewed as necessary.

2. Scope

- 2.1 This top level Protocol sets out the principles for information sharing between partner organisations. See appendix 1.
- 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. The considerations, though less stringent, must consider factors such as commercial or business, sensitive data, and the effect of many data sets being applied.
- 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 the secure information is securely transferred and that information shared is for justifiable 'need to know' purposes. See 6.3 and 11.6.

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:

- apply the Information Commissioner's Code of Practice's 'Fair Processing' and 'Best Practices' Standards
- follow, or demonstrate a commitment to, achieving the appropriate compliance with the Data Protection Act 1998. See appendix 2.
- develop local information sharing agreements that specify transaction details. See appendix 4 for template.

3.4 All partners are expected to promote employee awareness of the major requirements of information sharing. Appropriate guidelines will be produced where required to support this. They will be available to all employees through the partners' Intranet sites and through other communication methods.

4. The legal framework

4.1 Here is the principal legislation concerning the protection and use of personal information listed below, further explained in Appendix 2.

- 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.

5. Data covered by this protocol

- 5.1 All personal and anonymised information as defined in the Data Protection Act 1998 - DPA. **Anonymous** data should be used wherever possible.

Personal Information

- 5.2 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 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.
- 5.4 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.
- 5.5 An individual may consider certain information about themselves to be particularly 'sensitive' and may request other data items to be kept especially confidential. For example, any use of a pseudonym when their true identity needs to be withheld to protect them.
- 5.6 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.

Anonymised data

- 5.7 Make sure that anonymised information **does not** identify an individual, either directly or by summation.
- 5.8 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 data sources held by a partner to produce personal identifiable data.
- 5.9 Anonymising data does not remove the duty of confidence.

6. Purposes for sharing information

- 6.1 Information should only be shared for a specific lawful purpose or when appropriate consent has been obtained.
- 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 organisation 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 2.
- 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) as defined in the relevant information sharing agreement. 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 and so on.
- 7.3 It is recognised that Partners' organisational policies and procedures may place additional restrictions on the sharing of information. For example, limitations for the electronic transfer of information where secure communications cannot be guaranteed.

8. Consent

- 8.1 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 2 and 3 contain more information and the glossary may also be helpful.
- 8.2 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.
- 8.3 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.
- 8.4 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.
- 8.5 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.
- 8.6 Specific procedures apply when the data subject is under the age of 16 or if they do not have the capacity to give informed consent. In these circumstances, referral should be made to the relevant policy of the partner organisation.

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. See Appendix 2.
- 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 - process
- 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.

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 should be used together with local service level agreements, contracts or any other formal agreements that exist between the partner organisations.
- 11.4 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.
- 11.5 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.
- 11.6 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 and Derbyshire Information Access Group** will formally review this agreement 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 2

Relevant Legislation

1. Data Protection Act 1998

- 1.1 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.
- 1.2 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.
- 1.3 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.

1.4 The eight key principles of the Act are:

The Data Protection Act 1998	
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

- 1.5 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.
- 1.6 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.
- 1.7. 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.
- 1.8. Further advice is in BS 7799 and ISO/IEC Standard 17799.
- 1.9. 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

- 2.1 Conditions for processing personal data are that one condition in Schedule 2 should be met.
- 2.2 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
<p>The data subject has given consent, or the processing is necessary for:-</p> <ul style="list-style-type: none">• 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.	<p>The data subject has given explicit consent, or the processing is necessary for:-</p> <ul style="list-style-type: none">• 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

- 3.1 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.
- 3.2 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.
- 3.3 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.
- 3.4 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'.
- 3.5 In addition, all convention rights must be secured without discrimination on a wide variety of grounds under article 14.
- 3.6 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?
- 3.7 Article 8.1 provides that 'everyone has the right to respect for his private and family life, his home and his correspondence.'
- 3.8 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

- 4.1 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

- 5.1 The Freedom of Information Act 2000 applies to all public organisations and started coming into force in 2003.
- 5.2 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.
- 5.3 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

- 6.1 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.
- 6.2 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.

Appendix 3

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.

Information Sharing Agreement – the local information sharing agreement based on the template in Appendix 4.

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 fifteen 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 now covered 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 4

Information sharing agreement template

Partners

- 1.1 *Add the names of the partner organisations involved with this specific information sharing need.*
- 1.2 It will be the responsibility of these signatories to make sure that they:
 - have realistic expectations from the outset
 - maintain ethical standards
 - have a process by which the flow of information can be controlled
 - provide appropriate training
 - have adequate arrangements to test compliance with the agreement
 - meet Data Protection and other relevant legislative requirements.

Purpose of this information sharing agreement

- 2.1 Add a clear statement of why there is a need to share information between the organisations who are part of this Information Sharing Agreement, together with any relevant legislation or central government circulars that enable lawful data sharing.

For example

1. The purpose of this Information Sharing Agreement is to co-ordinate the continued care between the partner organisations.
2. This information sharing is done under the legal framework contained in the Children's Act 1998.

The type and extent of information to be shared

3.1 Routine information sharing

The information shared should be the minimum amount necessary. The agreement should clearly state what information is shared routinely. You should expressly state what information you are exchanging under this agreement.

For example

The information exchanged routinely is client name, address, and date of birth.

3.2 Anonymised information

Whenever possible data should be anonymised. If large volumes of data are provided for research and/or planning by partner organisations, as a matter of courtesy the outcome of that research/planning should be provided to the organisation(s) supplying the data.

3.3. How the information may be used

Add a clear statement of:

- what information is collected
- how it will be used and stored
- with whom it will/may be shared.

Data Quality

4.1. Agreement should be reached on how data quality issues will be addressed.

4.2 Information discovered to be inaccurate, out-of-date or inadequate for the purpose should be notified to the Data Controller who will be responsible for correcting the data and notifying all other recipients of the information who must ensure the correction is made.

Data retention, review and disposal

5.1. The partner organisations should agree an acceptable time period for the data to be exchanged.

5.2. They should also agree the time scales for retaining electronic and paper based information and how the information should be securely disposed of.

Appropriate Security

General

6.1 The partners to this agreement acknowledge the security requirements of the Data Protection Act 1998 applicable to the processing of the information subject to this agreement.

6.2 Each partner will make sure they take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

6.3 In particular, each partner must make sure they have procedures in place to do everything reasonable to:

- make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport

- deter deliberate compromise or opportunist attack
- dispose of or destroy the data in a way that makes reconstruction unlikely
- promote discretion to avoid unauthorised access.

6.4 Access to information subject to this agreement will only be granted to those professionals who 'need to know' to effectively discharge their duties.

Additional arrangements

7.1 To determine what security measures are appropriate in any given case, partners must consider the type of data and the harm that would arise from a breach of security. Information obtained in confidence may be regarded as requiring a higher level of security. In particular, they must consider:

- where the information is stored
- the security measures programmed into the relevant equipment
- the reliability of employees having access to the information.

Complaints and breaches

8.1 All complaints or breaches relative to this agreement will be notified to the designated Data Protection Manager of the relevant organisation in accordance with their respective policy and procedures.

8.2 Partner organisations should consider how they:

- tackle any breach of agreement
- handle internal discipline
- monitor security incidents
- deal with malfunctions.

Indemnity

9.1 The partner or third party processor will accept total liability for the breach if legal proceedings are served in relation to the breach.

Subject access requests

10.1 Explain how subject access requests will be processed.

- How will you deal with Subject Access Requests?
- Procedures for obtaining third party consent

10.2 Release of third party information

Consider:-

- how you will release information
- appropriate security of transfer of information
- safe havens.

General operational guidance

11.1 Resource implications

Partner organisations must consider the staff time and resource implications that are involved for the Data Controller extracting the data. If a request is made and then the data is no longer required there should be a process for withdrawing the request.

11.2 Appropriate signatories

Consider:-

- a named individual to lead on the Information Sharing Agreement
- who will champion training in the Information Sharing Agreement
- who will monitor the Information Sharing Agreement.

11.3 Review of the Information Sharing Agreement

Consider:

- how long the Information Sharing Agreement will last
- when will the Information Sharing Agreement be reviewed (insert date)

11.4 Compliance with the agreement

Consider how are you going to ensure compliance with the Information Sharing Agreement.

Closure/termination of agreement

12.1 Any partner organisation can suspend the Information Sharing Agreement for 30 days, if they feel that security has been seriously breached.

12.2 They must notify termination and/or completion that must be given in writing with at least 30 days' notice.

Consider:-

- termination and completion of agreement
- what will happen if there is a serious breach of confidentiality - does a termination or notice penalty apply.