

# A GENERAL FRAMEWORK FOR INFORMATION SHARING IN NORTH YORKSHIRE AND YORK

VERSION 2.0 2009



Developed by the ISA Project [isa@northyorks.gov.uk](mailto:isa@northyorks.gov.uk)



# Contents:

<b>Information Sharing Community</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
<b>Level 1 Strategic Overarching Protocol</b>	<b>9</b>
1.0 Purposes for which the information will be shared	10
2.0 Information Management	10
3.0 The Legal Framework	14
4.0 Principles Underpinning the Exchange of Information	14
<b>Level 2 Operational Protocol</b>	<b>20</b>
5.0 Operational Guidance	21
6.0 Obtaining Consent	21
7.0 Recording Consent	26
8.0 Staff Guidance on Seeking Consent	27
9.0 Making Disclosure with Consent	28
10.0 Making Disclosure without Consent	29
11.0 Determining Access to Personal Information 'The Need to Know'	30
12.0 Access, Storage and Security Procedures: General	31
13.0 Indemnities	34
14.0 Research and Planning	35
15.0 Individual's Rights	34
16.0 Breaches of Protocol	37
<b>Level 3 Protocol Management Procedures</b>	<b>38</b>
17.0 Protocol Management Procedures	39
18.0 Protocol Agreement	41
19.0 Certification	42
20.0 Level Three Protocol Requirements	42
<b>Annex A: The Legal Framework</b>	
<b>Annex B: Multi-Agency Consent Form</b> (for situations where consent is needed)	

# Information Sharing Community

The following organisations are committed to the General Framework for Information Sharing under the Governance Arrangements of the North Yorkshire Children and Young People's Strategic Partnership:

- Barnardos
- City of York Council
- Connexions York and North Yorkshire
- Craven District Council
- Hambleton District Council
- Harrogate Borough Council
- HMYOI Northallerton
- North Yorkshire and York Primary Care Trust
- North Yorkshire Children's Fund
- North Yorkshire County Council
- North Yorkshire Police
- North Yorkshire Police Authority
- North Yorkshire Probation Service
- North Yorkshire Youth Offending Team
- NSPCC
- Richmondshire District Council
- Ryedale District Council
- Scarborough District Council
- Selby District Council
- South Tees Acute Trust
- Sure Start
- The Learning and Skills Council
- The North East and North Lincolnshire Strategic Health Authority
- York Hospitals NHS Trust

# Introduction to the General Framework for Information Sharing

## Introduction

Information sharing refers to the processing of information either on a one-off or ongoing basis between partners for the purpose of achieving a common aim.

Effective service provision relies on the organisations communicating and sharing information with a wide range of partners. Information sharing is, therefore:

- A two-way process that enables links to be made between people, objects, locations and events that would not be possible otherwise;
- Can help deliver improved public services;
- Leads to an increased openness among partners which, in turn, builds confidence and trust;
- Increases expertise, professionalism and an understanding of the process of sharing information;
- Enables partners to make informed decisions about how best to protect and serve the public.

However, while there are clear advantages in sharing information with others, information should not be shared purely as a matter of routine. Each case must be viewed individually with informed decisions made about whether to share or not.

The sharing of information can be summarised in three distinct groups:

- Those required by or under statute (statutory obligation)
- Those permitted by or under statute (statutory power)
- Those made under common law to support the delivery of services including information sharing and dissemination

This Framework is consistent with the Guidance issued by HM Government and entitled 'HM Government Information Sharing Guidance' issued in October 2008.

<http://www.everychildmatters.co.uk/deliveringservices/informationsharing/>

The guidance includes:

Information Sharing: Guidance for practitioners and managers - giving practitioners clear practical guidance, drawing on experience and the public consultation.

Information Sharing: Pocket guide - a summary of the key decision-making considerations (see below for printing instructions).

Information Sharing: Case examples - a set of case examples which illustrate information sharing situations

Information Sharing: Further guidance on legal issues - a summary of the laws affecting information sharing in respect of children and young people. Please note this version is based on the 2006 guidance. An updated version will be available early in 2009.

Information Sharing: Endorsements and statements details of organisations who have formally endorsed the guidance and what they have said.”

Information Sharing Agreements (ISAs), also known as Information Sharing Protocols, should be used when sharing information with other organisations. An ISA is simply a formal arrangement between organisations who wish to share personal information which must be held and managed within each organisation. Establishing ISAs with partners have a number of advantages. In particular, they:

- Ensure consistency in the way information is shared;
- Allow the organisations to place conditions on the way information will be handled by the partner agency and vice versa;
- Ensure that information can be shared lawfully;
- Can help to build confidence in public organisations to protect and serve the public.

## **Background**

In order to support the development of effective protocols across North Yorkshire a multi-agency Information Sharing Framework has been established. This document provides a framework for the secure and confidential sharing of information between the subscribing organisations, enabling them to meet the needs of the local population for care, protection and support in accordance with national and local policy and legislative requirements.

### **The Three-Level Framework:**

The document is divided into three principle sections. Level I is a high level overarching protocol, which establishes principles. It is intended mainly for senior managers. Operational issues and purposes are in Level II; together with the two detailed annexes, is mainly aimed at team leaders and front line staff. Level III provides detail on specific arrangements which define the

processes by which information can and will be shared. All staff may have an interest in this section, especially those working already in joint teams. Level II and level III are templates to enable any of the organisations who are signed up to level I to utilise these to develop their own protocols for whichever information sharing partnership.

#### Level 1: Strategic Overarching Protocol

At the highest level, all organisations agree a common set of principles under which they may share information. This agreement, or overarching protocol, commits those who sign it to only sharing information lawfully and effectively at all levels of their organisation. It defines the general parameters against which all requirements for information sharing are measured, and outlines the way in which underlying levels in the model will be managed and monitored. All organisations sign up to the framework, the principles being ratified and owned at a high level of their organisations

#### Level II: Template Managerial Protocol

This document begins to define a greater level of detail. Not all organisations will need to subscribe to all purposes. Not all organisations signing the overarching protocol will be members of every information partnership. Examples of purposes to be included in the second level might be crime and disorder investigation and reduction, social inclusion or protecting the vulnerable. This document contains the information on consent, determining the need to know, access and security procedures, research and planning, individual rights and breaches of protocol.

#### Level III: Template Protocol Operational Procedures

This document consists of detailed, specific information sharing agreements. These agreements between individual organisations define how the information will be exchanged and monitored, methods of auditing and the details of the information to be shared. They will identify the routes through which requests for information may be made, the methods of auditing who has access to what, and the details of the information to be shared. This is a template to be completed by individual information sharing partnerships, these detailed agreements allow for local variation while maintaining the integrity of the information required.

Many of these third level agreements may already be in place, either formally or informally reflecting established practice and meeting daily needs. Although some work will need to be done to review current practice and lay out the agreements in consistent format, the use of the framework will allow organisations to build on existing arrangements and focus on identified gaps. Examples of the processes to be covered in third level agreements might be adult abuse, young offenders and teenage pregnancy.

## **Summary**

This three level framework allows operational staff to be given clear and unambiguous guidance over what can and cannot be shared with any specific partner. It enables organisations to build on existing practice, and allows flexibility for future development.

# **LEVEL I: STRATEGIC OVERARCHING PROTOCOL**

## **Overarching Information Sharing Protocol: Table of Contents**

### **Strategic Principles**

#### **1.0 Purposes for which Information will be Shared**

#### **2 Information Management**

2.1 Legitimate Basis for Obtaining and Using Information

2.2 Retention of Information

2.3 Accuracy

2.4 Relevance and Review

2.5 Recording Sources of Information

2.6 Transmitting Personal Information

2.7 Records Management

#### **3 The Legal Framework**

#### **4 Principles Underpinning the Exchange of Information**

## **STRATEGIC PRINCIPLES:**

### **1.0 Purposes for which Information will be Shared**

1.1 Information that is held and may be shared must have been obtained fairly and processed lawfully. It should be accurate, up to date and relevant to the purpose of sharing. The following is a list of partnerships that this protocol covers (this framework encompasses and supersedes existing protocols in these areas):

- Community Safety
- The delivery of integrated Health and Social Care Services
- The management and planning of services
- Integrated Processes for Children's Services
- Crime and Disorder Reduction

(Others will be added over time)

1.2 Specifically, information may be shared between organisations for the following purposes:

- Provision of appropriate care services
- Improving the health of people in the local community
- Protecting children, young people and adults
- Prevention and detection of crime
- Supporting communities (geographical or otherwise)
- Supporting people in need
- Investigating complaints and untoward incidents
- Managing and planning services
- Commissioning and contracting services
- Developing inter-agency strategies
- Performance management and audit
- Research
- Staff management and protection.

1.3 The purpose for the arrangement for exchanging information must be approved, understood and formally agreed by those entering into a partnership for this. Once the purpose has been decided agreed and documented, organisations must be decide whether it is necessary to share information in a personally identifiable form, or whether anonymised or statistical information would suffice.

### **2.0 Information Management**

#### **2.1 Legitimate basis for Obtaining and Using Information**

2.1.1 The first Data Protection principle requires that certain conditions are

met for processing information about individuals, including sensitive information such as racial or ethnic origin, physical or mental health, or criminal offences and proceedings.

- 2.1.2 To satisfy the requirements of the first Data Protection principle, the organisation's staff must follow the guidelines contained in this document and process information accordingly.
- 2.1.3 To ensure information is fairly obtained and processed, individuals must be given the following details at the time of obtaining their information:
  - The identity of the organisation who they're giving the information to
  - Where an individual is obtaining the information in person, they must ensure that they show appropriate identification from the organisation they represent
  - How their information may be used and who it may be shared with
  - A contact for further information (such as how an individual can check and/or correct their information, how to make a complaint)
  - Any other information necessary to ensure the obtaining is fair (such as who it may be disclosed to, the sources of the information)
- 2.1.4 All organisations party to information sharing protocols must ensure that the information processed is included on their Notification of Data Processing with the Information Commissioners Office. This will be evidenced by each organisation's Registration Numbers and Renewal Date, which should be recorded.
- 2.1.5 If information has been pooled for the purposes of an information sharing protocol, it will be established which organisation/s are the data controller/s for that information. The data controller/s alone should have responsibility for collecting and disclosing information on a need-to-know basis and be responsible for storing the information safely and limiting access.
- 2.1.6 Information sharing protocols should state at the start the consequences of exchanging or not exchanging information with others.
- 2.1.7 All organisations should ensure that they have in place a named senior officer or professional e.g. a solicitor, to enable staff to seek advice wherever they have any doubt about whether the information should be stored, disclosed or collected
- 2.1.8 Where an organisation employs another organisation to process personal information on its behalf, a written contract must be in place to ensure that the information governance meets the standards required by this framework.

## **2.2 Retention of Information**

- 2.2.1 Information must not be kept for longer than is necessary. There must be a legal justification to retain information, and not hold it just in case it may come in useful some day. Statutory and agreed discretionary retention periods will be observed. Where in integrated services / teams one agency has longer retention periods records should be kept for the longest retention period. When retention periods are met information must be securely disposed of.
- 2.2.2 Proper arrangements for the secure storage of all records including those records that are closed and required to be kept until the end of their retention periods.
- 2.2.3 Arrangements must be made about the retention and transfer of records about individuals who no longer fit the age criteria for that team (for example, when children transfer into adult services).

## **2.3 Accuracy**

- 2.3.1 The information held must be accurate and kept up to date. Steps must be taken to validate information, such as checking with the person who originally provided the information, if there is doubt as to its accuracy.
- 2.3.2 If any inaccuracies are found, that are a matter of fact, within any information then the organisation responsible for the information will need to take appropriate steps to amend the details and inform partners who have been given the information of the changes<sup>1</sup>.
- 2.3.3 If the individual has informed the organisation that they disagree with an opinion recorded, then the opinion should be reviewed.
- Where it is agreed that the opinion should be amended this should be recorded in the record along with the original opinion and the organisation must inform relevant partners.
  - Where the organisation still feels the opinion is correct, a record should be made of the disputed opinion and the reasons why it has not been changed and the organisation must inform relevant partners.

---

<sup>1</sup> Although note that when responding to a Subject Access Request, a signatory data controller may acknowledge an error rather than correct it, in accordance with its own procedure

## **2.4 Relevance and Review**

- 2.4.1 All information held must be adequate, relevant and not excessive in relation to the purpose(s) for which it is processed.
- 2.4.2 When sharing information sufficient information should be provided to the partner agency to ensure that it is meaningful without making it difficult to read or understand.
- 2.4.3 Information will undergo a form of evaluation appropriate to the purpose for which the information was collected and recorded. All information will be evaluated to determine its provenance, accuracy, continuing relevance to the purpose and what action should be taken. Provenance is the ability to determine the reliability and credibility of the source, and the value of the content of the information.

## **2.5 Recording Sources of Information**

- 2.5.1 Where information is obtained either in writing or electronically, the source of the information will also be clearly recorded and whether or not it is opinion. Where the information is opinion, the justification for arriving at that opinion should be recorded.
- 2.5.2 Where information is recorded organisations should agree a standard format for recording and storing the information, and use appropriate data standards.

## **2.6 Transmitting personal information**

- 2.6.1 Whenever possible use pseudonymised or anonymised information.

## **2.7 Records Management**

- 2.7.1 The management of records is fundamental to effective information management. The integrity of information relies on it being trusted, acceptable, useable and available. To assist the evaluation, actioning, sharing and review of information, the information must be in a format that is manageable, whether as an electronic, photographic or paper record.
- 2.7.2 The purpose of records management is to ensure that information is documented and maintained in such a way that its evidential weight and integrity is not compromised over time. To achieve this, records need to be managed throughout their lifecycle from creation to disposal. This process will involve the audit and maintenance of records to enable them to remain useful. This will also enable the discharge of legal responsibilities.

### **3.0 The Legal Framework and Guidance**

3.1 Operating within the legal framework rests on proper interpretation of the legislation and the extent and scope of the administrative powers (vires) of the organisation. Examples of key legislation and guidance currently relevant to information sharing are listed below, and outlined in Annex A (Working Document)

- Access to Health Records Act 1990
- Children Act 1989
- Children Act 2004
- Children [Leaving Care] Act 2000
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Criminal Justice Act 2003
- Criminal Procedures and Investigations Act 1996
- Data Protection Act 1998
- Education Act 1996
- Freedom of Information Act 2000
- Homelessness Act 2002
- Housing Act 1996
- Human Rights Act 1998
- Local Government Act 2000, 1972
- Mental Health Act 1983
- Mental Health Act 2007
- NHS & Community Care Act 1990
- Race Relations (Amendment) Act 2000
- Regulation of Investigatory Powers Act 2000
- The Learning and Skills Act 2000
- The Protection of Children Act 1999

3.2 Case law, including international case law, will also inform the legal position on aspects of information sharing.

### **4.0 Principles Underpinning the Exchange of Information**

In seeking to share personal information about individuals, the organisation(s) will abide by the following principles.

#### **4.1 General Principles**

4.1.1 The organisations recognise that most initiatives requiring a multi-agency approach cannot be achieved without the exchange of information about individuals, levels of activity, the level and nature of resources and about their approach to addressing the issues. Their adoption of a multi-agency approach to address issues, therefore, includes a commitment to enable such information to be shared when

appropriate. Organisations must also make arrangements as to who will collect store and disclose the relevant information.

- 4.1.2 The organisations are fully committed to sharing information in accordance with their statutory responsibilities and in compliance with the Data Protection Act 1998, Section 8 of the Human Rights Act 1998, the Freedom of Information Act 2000, all other relevant law, any relevant internal codes of practice and the principles of the Information Charter (included at Annex A)
- 4.1.3 Personal information will be deemed to have been provided in confidence when it appears reasonable to assume that the provider of the information believed that this would be the case. It is generally accepted that most, if not all, information provided by individuals to organisations including social care and health organisations is confidential in nature.
- 4.1.4 The first principle of the Data Protection Act 1998 requires that personal data must be processed fairly and lawfully.
- 4.1.5 The information will only be shared if there are legal grounds for doing so and an appropriate condition of Schedule 2 (and Schedule 3 in the case of sensitive personal data) of the Data Protection Act 1998 can be demonstrated.
- 4.1.6 Organisations will put into place individual second and third level protocols that demonstrate in detail the principles described in this document.

## **4.2 Confidentiality**

- 4.2.1 The organisations that are party to this document accept the duty of confidentiality and will not disclose personal information without the consent of the person concerned, unless there are statutory grounds or other demonstrable overriding justifications for so doing.
- 4.2.2 Organisations will use information disclosed to them under an agreed protocol only for the specific purposes set out in the protocol.
- 4.2.3 Information shared with a member of another organisation for a specific purpose will not be regarded by that organisation as intelligence for the general use of the organisation.
- 4.2.4 The duty of confidentiality only applies to identifiable information and not to aggregated data derived from such information or to information that has otherwise been effectively anonymised or pseudonymised
- 4.2.5 In requesting release and disclosure of information from members of partner organisations, staff in all organisations will respect the duty of confidentiality and not seek to override the procedures that each

organisation has in place to ensure that information is not disclosed illegally or inappropriately.

### **4.3 Consent**

4.3.1 The organisations that are party to a protocol accept that where consent is required to share information, for that consent to be valid, the person concerned must have the capacity to make the decision, have received sufficient information to make a decision and not be under duress. The issue of consent is such an important and complex one that there is a detailed discussion of issues arising in Level II of the Information Sharing Protocol. This covers the definition of consent.

### **4.4 Lawful purpose**

4.4.1 Although consent is an important part of lawful purpose, it is not necessarily enough on its own.

4.4.2 Organisations that are signatories to this protocol framework will ensure that they have the appropriate statutory authority by referring briefly to the vires or implied powers and any statutory gateways that are being relied upon. Organisations should also state whether they are obliged to or are merely enabled to exchange information for all their services which involve information sharing.

4.4.3 All protocols should meet the first and second principles of fairness and lawfulness required within the Data Protection Act 1998.

### **4.5 Subject Access Rights**

4.5.1 Each party for the protocol will devise its own procedures to ensure data subjects' rights are observed.

4.5.2 Individuals have the right to see a copy of the information that is held about them, subject to limited exemptions, whether it is in electronic, paper or any other form.

4.5.3 They also have the right to apply to the Court for an order requiring the organisation to rectify, block, erase or destroy information relating to them that is inaccurate, as well as any expressions of opinion that are based on inaccurate information.

4.5.4 There is more detailed information on Subject Access Rights in Level II of the Information Sharing Protocol.

### **4.6 Need to know**

4.6.1 Where it is agreed that personal data will be shared, it will be shared only with those who need to know, and only that information which is

needed will be shared.

4.6.2 The Level II document details how to determine the 'Need to Know'

#### **4.7 Time Period over which Consent Applies**

4.7.1 The consent request needs to make clear how long the consent applies, and under what circumstances, which means in practice also that the consent given will need to be reviewed by the agency or organisation from time to time under an agreed regular procedure which applies to all such consents. Consent for one purpose does not imply consent for another.

#### **4.8 Complaints procedures**

4.8.1 The organisations are committed to having procedures in place to address complaints relating to inappropriate disclosure or failure to disclose personal information. Individuals will be provided with information about these procedures. Complaints about the use, or disclosure, of personal information should be addressed by the organisation where the complaint originated. If the complaint affects more than one partner organisation it should be brought to the attention of the Data Protection Officer/s or other appropriate officer/s who should liaise with their opposite numbers to investigate the case.

#### **4.9 Staff Compliance and Vetting**

4.9.1 Organisations will ensure that all staff who work with individual's information understand and comply with their responsibilities to share information in accordance with agreed protocols.

4.9.2 Where the sensitivity of the information requires that staff in one organisation must go through a vetting process (for example CRB or enhanced CRB checks) where vetting is justified, then staff from other organisations that have access to the information should be subject to the same vetting procedures.

4.9.3 The actual Level Three agreement with other parties will specify what guarantees and evidence are required appropriate to the sensitivity of the information which is subject to the agreement.

#### **4.10 Disciplinary Action**

4.10.1 Organisations will ensure that staff codes of conduct, contracts of employment and performance reviews make reference to the disciplinary action which will be taken should staff disclose information about a person inappropriately or on a basis which is not supported in agreed protocols.

## 4.11 Data Integrity

4.11.1 Data quality is fundamental to successful information management. It is essential that all information is recorded properly at the outset. Failure to get it right at the outset will lead to further work and an increased likelihood of missing a potentially vital link. High quality information helps to ensure that appropriate action is taken, means that information is shared where appropriate, and that it can be retained for the appropriate time length.

4.11.2 All information must conform to the following data quality principles:

- **Accurate** – care must be taken when recording information and, where appropriate, the source of the information must also be recorded. If there is any doubt over the authenticity of the information clarification must be sought from the source. Procedures for checking that information is of good quality prior to it being shared must be in place. Inaccurate information must be corrected by all organisations as soon as possible. Where an organisation discovers that they have shared inaccurate information, they must not only correct their own records, but should make sure that the information is also corrected by the other organisation(s) they have shared the information with. In ensuring accuracy it is important not to delete historic information that may be significant (such as details of previous addresses).
- **Adequate** – recorded information must be accurate, sufficient and not excessive for the purpose in which it is processed. The nature of the event will determine the information that is relevant. All recorded information must be easily understood by others.
- **Relevant** – information recorded must be relevant to the purpose. Opinions need to be clearly distinguished from fact.
- **Timely** – information must be promptly recorded in accordance with the agreed timescales.

4.11.3 When disclosing information about an individual, professionals will clearly state whether the information, or any part of it, is fact or opinion. Where it is opinion, the reasons for that judgement will be stated

## 4.12 Requests from Professionals to Keep Information Confidential

4.12.1 Where professionals request that information supplied by them be kept confidential from the individual, they must submit a justifiable reason which can and will be tested for appropriateness before a decision is made to grant or deny the request. The reasons for this decision should be recorded.

## **4.13 Raising Awareness**

4.13.1 In order to ensure that consent to the sharing of personal information is informed, all organisations will have available material explaining:

- The rights of individuals under the Data Protection Act 1998, particularly in relation to sensitive personal data
- Details of the procedures in place to enable individuals to access their records.
- Details of the circumstances under which information may be shared without consent and the procedures which will be followed.
- Details of the complaints procedures to follow in the event that the individual concerned believes information about them has been inappropriately disclosed.
- Details of how the information they (the individual) provide will be recorded, stored and the length of time it will be retained both by the point of contact agency or organisation and the organisations to whom they may disclose that information.
- Where practicable, details of the length of time for which consent to particular disclosure is valid.

## **4.14 Deceased People**

The Data Protection Act 1998 applies only to information about living persons. Therefore information held on the deceased is not personal information, as defined by the Act. However, the duty of confidentiality to the deceased may continue to apply. Therefore parties to the protocol, when developing protocols, will apply these to deceased people as well as living people.

# **LEVEL II: OPERATIONAL PROTOCOL**

## **Operational Protocol: Table of Contents**

### **Template for managerial and operational staff for developing second level inter-agency information sharing protocols**

- 5.0 Operational Guidance
- 6.0 Obtaining Consent
- 7.0 Recording Consent
- 8.0 Staff Guidance on Seeking Consent
- 9.0 Making Disclosure with Consent
- 10.0 Making Disclosure without Consent
- 11.0 Determining Access to Personal Information 'The Need to Know'
- 12.0 Access, Storage and Security Procedures: General
- 13.0 Indemnities
- 14.0 Research and Planning
- 15.0 Individual's Rights
- 16.0 Breaches of Protocol

## 5.0 OPERATIONAL GUIDANCE

- 5.1 The following sections outline the requirements that will be common to all second level information sharing protocols where personal information is being shared. Where non personal information is shared then only use the appropriate sections as consent is not required. Second level protocols e.g. for Integrated Processes for Children's Services will define detailed responsibilities and arrangements and will comply with the principles in the overarching protocol in Level I of this document and the guidance in this section. Some second level protocols may include additional specific requirements arising from the particular requirements of a specific partnership.
- 5.2 It is recommended that a standard consent form and arrangements set out in Level II in relation to Consent are used by the organisations who are signed up to the overarching protocol in Level I of this document. The standard consent form is attached at Annex B. However, should organisations involved in developing second level information sharing protocols wish to amend the standard consent form at Annex B for their own requirements they may do so.
- 5.3 In addition organisations who are signatories to the overarching protocol in Level I will develop a strategy to inform the public of their rights and the requirement to seek their consent to share and obtain their personal information with other organisations in order to fulfil their statutory responsibilities.
- 5.4 Where the sensitivity of the information requires that staff in one organisation must go through a vetting process (for example CRB or enhanced CRB checks) where vetting is justified, staff from other organisations that have access to the information must be subject to the same vetting procedures. Appropriate checks to ensure the required vetting processes have taken place must be evidenced and documented prior to information sharing taking place.

## 6.0 Obtaining Consent

- 6.1 This section applies to all sharing of personal information; however there are some circumstances where consent is **not** required to share information. When it is appropriate to do so individuals should be informed that their information will be shared. The following situations **do not** require consent to share information, but should be addressed on a case-by-case basis to identify why it was not felt appropriate to obtain consent. (See also 6.3 – 6.13, and 10)  
Where operational staff are of the view they require further advice and/or authorisation, they should obtain this from a named senior officer or solicitor within their organisation.

- If you have a statutory duty to share the information, or where instructed to do so by a court
- When an individual is believed to be at risk of significant harm
- Where there is evidence of serious public harm, or risk of harm to others
- Where there is evidence of a health risk to an individual
- For the prevention, detection or prosecution of serious crime
- Sharing anonymised or non-person identifiable information

6.2 Organisations will train relevant staff in the obtaining of consent and information security.

**The following covers areas where consent is or may be required to share information**

6.3 Where consent is required, it has to be informed, specific and fair. Protocols should include procedures for obtaining consent within the law.

6.4 Consent will normally be sought at the first contact with the person concerned using the standard consent form at Annex B unless the individual is unable, at that time to fully comprehend the implications or make an informed judgement. A risk assessment would be undertaken to determine if, in the professional judgement of the staff member(s), it would be detrimental to the health of the person to address these issues at first contact, then the decision not to proceed with seeking consent will be documented along with the reason, and the arrangements for completing the process. The individual should also be advised that their information will only be shared without their consent in exceptional circumstances. These exceptional circumstances can override consent and can include the situations at 6.1 (above)

6.5 Written consent should also be obtained once a year, or where appropriate as long as consent is regularly reviewed. In addition, where possible, written consent should be obtained should a particular situation arise, which may be unforeseen or unusual and which requires consent to disclose specific information, which is not covered by the last consent form.

6.6 If it is thought that the individual does not have the capacity to make an informed decision, the guidance at 6.14 (Establishing Fitness to Give Consent) will be followed.

- 6.7 It will be explained to the individual the purpose for which the information is being collected and what information is likely to be collected, where it will be stored (electronically and manually and on other media), how it may be used, who it may need to be shared with and why.
- 6.8 The individual will be informed that they can choose to limit both the type of information that will be shared and the organisations with which it can be shared.
- 6.9 The individual should be advised that they can refuse to give their consent or withdraw their consent to the sharing of information at any point during assessment or provision of services.
- 6.10 The individual must be aware that she or he can exercise this right to limit refuse or withdraw their consent and that, should they do so, they will be informed of any potential impact on service delivery.
- 6.11 Where consent is refused, withdrawn or limited this should be recorded (see 7.5) and each organisation must abide by the refusal or withdrawal of consent or any limitations on consent
- 6.12 Individuals will be told that they have a right to request their records and to amend any information that is factually incorrect.
- 6.13 The individual will be informed that if information they provide about them is anonymised, it can be shared with other organisations for statistical or planning purposes, without their consent. It will be made clear to the individual that the information will be anonymised in such a way that they could not be identified by it.

#### **6.14 Establishing Fitness to Give Consent**

- 6.14.1 "Consent" is defined in the EU Data Protection Directive (95/46/EC) 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".
- 6.14.2 The use of the word "signifies" above means that there must be some sort of active communication between the parties. The consent must also be given on an informed basis i.e. the person knows what they are consenting to.
- 6.14.3 If it is proposed to share personal information in respect of a **young person** a judgement needs to be made in each case as to whether the child understands the nature of the request and therefore has the capacity to give consent. Where this is the case it is good practice to encourage them to involve their parents/guardians/carers in the decision making. If it is felt that the child is unable to understand then the parent(s)/guardian(s) /carer(s) should be consulted about consent.

6.14.4 **Adults** are always assumed to be competent to give consent unless it is demonstrated otherwise. If there is doubt about capacity this should be considered in relation to the requirements which are stipulated in the Mental Capacity Act 2005 for assessing capacity and obtaining consent where there is a lack of mental capacity to do so as follows:

6.14.5 **Assessing Capacity:**

If it appears that the individual lacks mental capacity to make informed decisions, capacity to be able to give consent can be assessed by considering whether the individual has the capacity to:

- understand the information relevant to the discussion?
- retain the information?
- use or weigh that information as part of the process of making the decision, or
- communicate his/her decision (whether by talking, using sign language or any other means)

**Lacking Capacity:**

Where an individual does not have the capacity to make an informed decision, decisions to disclose information can be made by considering:

Is there any person previously identified by the individual who is appropriate to consult and where it is practical to consult them, who could give an indication of the person's wishes about making any decision about disclosing information? Or:

- anyone caring for the person or interested in their welfare, or
- someone with Lasting Power of Attorney granted by the person which authorises them to make decisions about anything, or authorises them to make a decision about disclosing information, or
- anyone appointed for the person by the Court.

If there is not a person previously identified by the individual, consider (if known):

- the person's past and present wishes and feelings
- their beliefs and values

- other factors likely to be considered if she/he were able to do so.
- Staff should then form an opinion about consent and obtain the signature of the carer or representative or any other person consulted. Staff should explain to the person signing the consent form that they are signing this in relation to being consulted about whether they think the person would wish for his/her information to be disclosed. They are not being asked to provide consent on behalf of the service user.

#### 6.14.6 **Independent Advocacy - Independent Mental Capacity Advocate (IMCA).**

In the case of incapacity of a vulnerable individual over the age of 16, where there is a problem about how the 'person's best interests' should be agreed (for example, in disputes involving relatives), an independent advocate may have to be brought in.

The Mental Capacity Act 2005 requirements for the commissioning of Advocates and the appointment of people with Lasting Power of Attorney, include a requirement that where a person has been appointed under a personal welfare Lasting Power of Attorney that this person will determine if information can be disclosed to anyone. Staff must normally consult with a person with Lasting Power of Attorney where one has been appointed before sharing any information with anyone. Where it is not possible to consult, for example, because urgent treatment is necessary, staff must act in the individual's best interests and advise the individual of any action taken as soon as practicable.

Staff will need to record accurately the decisions they make about the assessment of mental capacity, and the determination of best interests. The decisions should be recorded.

Where a person lacks capacity and has no-one to support them with major, potentially life-changing decisions then staff in Health or Children and Adult Social Care Services are required to instruct an Independent Mental Capacity Advocate (IMCA) before making the decision. In England, Health and Adult and Children Social Care staff can use their discretion as to whether they involve an IMCA in a care review and in adult protection procedures.

The duties of an IMCA are to:

- support the person who lacks capacity and represent their views and interests to the decision maker.
- obtain and evaluate information.

- as far as possible, ascertain the person's wishes and feelings, beliefs and values.
- obtain a further medical opinion, if necessary.

6.14.7 If it is not practical to contact an individual to obtain consent, information may have to be shared, taking into account the person's best interests, to enable appropriate care to be provided. The information sharing and reasons for doing so should be recorded on the individual's record.

6.14.8 In the case of incapacity or of a vulnerable individual over the age of 16 where there is a problem about how the 'person's best interests' should be agreed (for example, in disputes involving relatives), an independent advocate's advice may have to be sought.

## 6.15 Checking On Whether Consent Already Exists

Whenever a new case or closed case is opened staff will check the individual's case file, notes or records (paper and electronic) for any documents recording consent and related information.

## 7.0 Recording Consent

**The Data Protection Act does not define consent but the European Union Directive EU DP Directive (95/46/EC) which led to this Act indicates that failure to respond to a request to give consent may not be taken as indicating consent, and that consent, once given, can be withdrawn. Explicit consent means in practice, signed consent, with no ambiguity and a full statement of the purposes for which consent is given.**

7.1 The consent form at Annex B, or an equivalent consent form, records consent and should be signed and dated by the individual concerned as well as the staff member. A copy will be made and given to the individual. Where consent is given verbally (for example if individuals give consent but refuse to sign) notes on the conversation around verbal consent will be carefully documented.

7.2 Details of obtaining the individuals consent should be entered on their records. E.g. case files, patients notes, pupils records, etc.

7.3 The consent form will be stored in such a way that they can be viewed with the individual's record (usually at the front of the case file, patients' notes, pupil's records etc).

7.4 Electronic systems should have the facility to record and retrieve details of consent.

7.5 If an individual limits the disclosure of information in any way, or refuses or withdraws their consent this will be flagged on their records in such a manner that any member of staff subsequently involved with that person, is alerted to the limitation of consent, and restricts access accordingly.

7.6 Consent to the disclosure of personal information for a particular purpose will be limited to that purpose.

## **8.0 Staff Guidance on Seeking Consent**

8.1 To ensure that consent seeking within the second level protocol is properly understood and that consent is sought in an appropriate manner, guidance for staff should include the obtaining of consent.

8.2 Organisations that are party to second level protocols should ensure their staff are aware of their responsibilities when seeking consent; they should be made aware of this guidance.

8.3 The guidance should give clear information on:

- the need to seek consent and the consequences of not doing so
- who is able to be consulted about consent on behalf of another person
- the circumstances under which information may be disclosed without consent
- who can authorise the disclosure of information without consent and how this authority should be requested. In many situations the advice of the Caldicott Guardian or someone very senior in the organisation may be required.
- the records which must be kept of the process of seeking consent
- the procedures for recording and storing consent to share information
- the procedures for recording limitations of consent to share
- the procedures to be followed when consent is limited.

8.4 Second level protocols will include a date by which all parties to the protocol will have this guidance in place and will set out how progress in implementing this guidance will be monitored.

## **9.0 Making Disclosure: With Consent**

- 9.1 A staff member receiving a request for personal information about an individual from a partner organisation will first check the individual's case file, notes or records (paper and electronic) for any documents recording consent and related information.
- 9.2 Members of staff without access to an individual's file must check any other relevant person before releasing information.
- 9.3 Particular care will be taken to ensure that consent to share sensitive personal data has been given explicitly in writing.
- 9.4 When disclosing information about an individual, organisations will indicate to what extent the information is current, factual or an expression of opinion, and whether it has been confirmed as correct by the individual.
- 9.5 The requesting organisation will only ask for information that is necessary, likewise the organisation disclosing information will ensure that the information requested is necessary – see 11. "need to know"
- 9.6 When personal information is shared with and obtained from another organisation, this should be noted in the individual's file. Accurate records will be kept of what information has been disclosed to whom, the source of the data disclosed, the date on which it was disclosed and the method of disclosure, e.g. verbal, by post, etc and the reason for the request. In these circumstances, the person making the decision will document the reasons in the individual's records; the individual should be given access to the reasons given.

## **10.0 Making Disclosure: Without Consent**

- 10.1 A decision to share information without consent will only be taken following due consideration of the circumstances of the case. Where staff are not sure whether to disclose without consent, they should seek the advice of a senior member of staff (e.g. the Caldicott Guardian if there is one in their organisation) or named individuals for staff to consult.
- 10.2 The decision to share personal information without the consent of the individual must be:
  - Fair – the decision to share information without consent will be based on necessity and not just on convenience or desirability and will seek to balance the rights of the individual against any wider considerations that may be relevant.

- Lawful – the organisation seeking to share information must have a relevant statutory power to be able to do this, for example the Children Act 1989
- Justified – it must meet one of the conditions under Schedules 2 (and 3 for sensitive personal information) of the Data Protection Act 1998. The most common are:
  - To comply with a legal obligation
  - To protect the vital interests of the individual. "Vital interests" means life or death circumstances and can involve some mental health situations, child or adult protection situations, potential physical assault, sexual offences or arson.
  - For the administration of justice, or the exercise of statutory functions, or the exercise of government functions or other functions of a public nature.
- For Schedule 3, the following are relevant:
  - Where it is necessary for the purposes of legal proceedings, legal advice, or establishing or defending legal rights.
  - For the sharing of data relating to racial and ethnic origin for equal opportunity purposes.
  - To protect the vital interests of the individual or another person.

10.3 In addition to the need to comply with the Data Protection Act 1998 there is a need to ensure that decisions to share without consent are consistent with either Article 8 of the Human Rights Act or the Common Law Duty of Confidentiality.

10.4 Article 8 of the Human Rights Act states that "everyone has the right to respect for his private and family life, his home and his correspondence." A number of exceptions to this right are detailed in the Article. These exceptions need to be in accordance with the law and "necessary in a democratic society" and are as follows.

- In the interests of national security or public safety
- For the prevention of disorder or crime
- For the protection of health or morals
- For the protection of the rights and freedoms of others

10.5 These are broad definitions and their specific application will only be determined over time on the basis of case law.

- 10.6 To justify use of any of them it is necessary to show **proportionality**: that a fair balance has been struck between the rights of the individual and the relevant justification.

Sharing personal information will be proportionate if:

- The individual concerned consents to the information being shared;
- The purpose justifies infringing the right to privacy;
- The measures taken to meet the purpose are rational and fair;
- The means used to share are no more than is necessary to accomplish the purpose.

- 10.7 Under the **Common Law Duty of Confidentiality**, personal information can be shared legitimately if it is anonymised or if consent has been given.
- 10.8 Organisations should ensure that there is an appropriate justification for sharing without consent, that there are no legal restrictions on sharing, for example The Human Fertilisation and Embryology Acts 1993, 2003.
- 10.9 Organisations should have arrangements in place to enable sharing without consent to be authorised in disaster situations, for example emergency planning arrangements.
- 10.10 If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure, any advice received prior to disclosure and the person(s) to whom the information was disclosed.
- 10.11 The individual should normally be informed of the disclosure made without consent. Only in circumstances where there are justifiable concerns for the safety of staff or other people will the decision not to inform the individual of the relevant disclosure be taken. In these circumstances, the person making the decision will document the reasons in the individual's records, though the individual should be given access to the reasons given when it is deemed to be appropriate to do so.

## **11.0 Determining Access to Personal Information: "The Need to Know"**

- 11.1 The access and security arrangements for the protocol reflect the principle that requests for information are specific and recorded and made on a "need to know" basis only. Where the staff are not sure, they should seek the advice of a senior member of staff (e.g. the Caldicott Guardian if there is one in their organisation) or named individuals for staff to consult.

- 11.2 Staff will only have access to information if the function they are required to fulfil at that particular point, in relation to a particular individual, cannot be achieved without access to the information specified.
- 11.3 For the purposes of a specific second level information sharing protocol access to electronic systems will be defined by staff role and the need to know specific elements of personal information. Controls will be defined for various staff roles and access provided accordingly.
- 11.4 Depending on levels of consent to sharing specific elements of sensitive data in electronic systems, it may be necessary only to allow access to designated senior staff.
- 11.5 Where personal data and sensitive personal data are contained in manual/ paper case files each organisation will have procedures in place to control access. These will include rules about where any sensitive data is recorded and stored. It may be stored separately, and subject to more stringent access rules.
- 11.6 In drawing up second level protocols for sharing information, partners will agree the "rules" for access by going through the following steps for each service area and documenting this.
- Identify the staff roles where there is a legitimate interest in sharing information.
  - Define the specific elements of information required for each role
  - Identify the reasons the information is required for each role

## **12.0 Access, Storage and Security Procedures: General**

- 12.1 The Data Protection Act 1998 applies to personal data held in both manual (usually paper) and electronic files, to any processing done on the personal data and requires that personal data be adequately protected, for example by an ISO 27001 risk assessment process. Whenever possible use pseudonymised or anonymised information.
- 12.2 It is necessary to control access to personal information and to ensure that it is securely held. This applies to both electronic and manual records. Each organisation should be able to describe and apply its own security measures to protect store and transmit the information it processes. Levels of access should be established to prevent unauthorised access to information. Common protective markings should be agreed and used (i.e. restricted, confidential) likewise each organisation should agree the standards for the storage and

transmission (using encryption technology where appropriate) of the information.

- 12.3 Organisations will ensure that all manual files, log books and other confidential information are 'tracked', kept in secure, controlled locations, with appropriate access controls based on the need to know principle.
- 12.4 Laptops, palm tops, PDAs, floppy disks, CDs and any other electronic devices, media or networks that hold and transfer personal data will be (using encryption technology) kept in secure, controlled storage when not in use. Access will be limited to appropriately authorised staff. Organisations will ensure that staff are instructed **not** to process personal or sensitive personal data on their own personal computers, as adequate security for that data cannot be guaranteed.
- 12.5 Organisations will ensure that procedures for maintaining security and confidentiality also apply in circumstances where workers are based in their own homes by ensuring they use the guidance within this protocol both at work and when working from home.
- 12.6 Confidential information must be inaccessible to any unauthorised persons, and not left even for short periods where they might be looked at by unauthorised persons. Confidential information should not be left unattended in vehicles, trains or modes of transport.

## 12.7 **Transfer of Information Verbally**

- 12.7.1 Much information sharing takes place verbally, typically between colleagues in a single organisation, but also between people in different organisations. Verbally sharing information is subject to the same legal and procedural regulations as others forms of sharing information. These conversations can occur in the privacy of an office, but can also take place at a worker's desk, in an open plan office , on the telephone, including mobile phones and in public places.
- 12.7.2 When information is to be shared verbally members of staff will ensure that confidentiality is maintained and that the rules regarding transferring information on a "need to know" basis are observed. This will normally mean that the relevant staff members move to an area where privacy can be guaranteed for the transfer of information. If this is not possible, the transfer of information will happen via another and more secure method.

## **12.8 Transfer of Information by Telephone and Mobile Phones**

12.8.1 Where information is to be shared by phone, the member of staff will ensure that the recipient is either known to them or properly identified. Where the recipient is not known to the member of staff and they (the recipient) has initiated the phone call, the member of staff will request the recipient's phone number (their organisation's reception or switchboard and not the recipient's direct number) and phone them back. Staff should take care when using mobile phones never to disclose information in a crowded environment where they might be overheard.

12.8.2 Messages containing confidential personal information should not be left on voice mail or answer machines

## **12.9 Transfer of Information by Fax**

12.9.1 The information will only be sent to a "Safe Haven" fax machine. A Safe Haven fax is one that is managed in such a way that security is enhanced. The safeguards include:

- The fax is sited in a secure room, or that access to the fax machine is controlled
- All organisations have written procedures for handling faxes which should be included in staff training.

## **12.10 Transfer of Information by Electronic Means**

12.10.1 Transfer of information electronically, including communications by internet and/or email is not secure and messages can be intercepted and read by someone else. Therefore personal information will **only** be transferred electronically where encryption methods and standards are in place and have been agreed by the signatories to the protocol, see 12.11.2.

12.10.2 Partner organisations will agree on encryption methods and standards.

## **12.11 Transfer of Information by Post**

12.11.1 Organisations must assess security adequacy of internal and external mail mechanisms. Adequate measures including 'double enveloping' and marking 'to be opened by addresses only' specific addressing by job title or named individual should be used.

12.11.2 Consider the use of couriers or recorded delivery

## **12.12 Storage and recording standards**

12.12.1 When using shared manual and or electronic systems to hold information for the purposes of the protocol, only information that is relevant to the purpose of the protocol should be held within that system.

12.12.2 When recording information organisations should agree a standard format for the collection and storage of that information and adopt common data standards. This will enable easier, more efficient exchanging and processing of data. It will also remove ambiguities and inconsistencies in the use of data.

## **13.0 Indemnities**

13.1 Each second level protocol will also include agreements that indemnify organisations for any action taken against them or their organisation as a result of the unauthorised use of confidential information by one of the other parties to the protocol.

## **14.0 Research and Planning**

14.1 Organisations in receipt of statistical data derived from individual records of partner organisations will request permission from the originating organisation if they wish to use that information for any purpose other than that for which the information was originally provided.

14.2 Individual protocols will also specify arrangements for the approval of the wider use or publication of case studies based on material collated for the specific purposes covered by the protocol and disclosure of information for research purposes.

14.3 Where organisations have an established Research Governance Frameworks for agreeing new research in place they should comply with these.

## **15.0 Individuals' Rights**

### **15.1 Subject Access**

15.1.1 Each party to the protocol will devise it's own procedure to ensure data subject's rights are observed.

15.1.2 Individuals have the right to request a copy of information held about them, with limited exemptions, whether it is held electronically or manually. Signatories to second level protocols must agree procedures as to how this right will be managed.

- 15.1.3 If they so request it, individuals must be given in permanent form, a copy of the information held about them, with a summary of the purposes for which the information is held, who it is obtained from, and who it is or may be disclosed to.
- 15.1.4 All requests for information from the data subject must be passed to a nominated person to ensure they are dealt with promptly and within established procedures.
- 15.1.5 A fee for each request for information can be charged, though it can also be waived.
- 15.1.6 Where the information contains identifiable details of a third party, the information may require editing to remove names or other identifying details. Only the minimum amount of alteration is permitted before the information is made available to the individual. Where the information cannot be disclosed without disclosing identifiable information about a third party, that third party's consent to the disclosure must be sought.
- 15.1.7 Where consent to disclose information relating to an identifiable third party individual, has been withheld or cannot be given, a decision will be made whether it is reasonable to comply with the request without the third party's consent. In making any such decision, regard will be given to:
- Any duty of confidentiality due to the third party
  - Any steps taken by the information owner with a view to seeking consent of the individual.
  - Whether the third party is capable of giving consent.
  - Any express refusal of consent by the third party.
- 15.1.7 Where the personal data is identified as belonging to a partner organisation and signatory to this protocol, it will be the responsibility of the nominated person to contact that organisation to determine whether the information can be provided to the data subject or must be withheld. Where information is to be withheld the reasons for withholding the information must be lawful and documented.
- 15.1.8 Individuals also have the right to apply to the Court for an order requiring the organisation to rectify, block, erase or destroy information relating to them that is inaccurate, as well as any expressions of opinion that are based on inaccurate information.
- 15.1.9 Individuals can appeal to the Information Commissioner or to the Courts about a decision not to disclose part or all of their records. However, they should contact the organisation in the first instance.

15.1.10 A court may also make such an order if any individual has suffered damage in relation to any of the requirements of the Data Protection Act 1998, and may require that third parties be notified if information has been disclosed to them.

## **15.2 Right to Prevent Processing Likely to Cause Damage or Distress**

15.2.1 An individual is entitled to serve upon an organisation a written notice requiring them to cease or not begin processing their information, where such processing is causing or is likely to cause unwarranted substantial damage or substantial distress to them or to someone else.

15.2.2 This right is unavailable where:

1. The data subject has given their consent to the processing (unless that consent has been withdrawn or limited), and/or
2. The processing is necessary:
  - (a) For the performance of a contract to which the data subject is a party or
  - (b) For the taking of steps at the request of the data subject with a view to entering into a contract
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by a contract.
4. The processing is necessary in order to protect the vital interests of the data subject or another individual or individuals

15.2.3 Signatories to individual second level protocols must agree procedures as to how this right will be managed.

## **15.3 Right to Prevent Processing for Purposes of Direct Marketing**

15.3.1 Individuals are entitled, by written notice, to require an organisation to cease or not to begin processing information relating to them for the purposes of direct marketing.

15.3.2 Signatories to individual second level protocols must agree procedures as to how this right will be managed.

15.3.3 Direct marketing is defined in the Data Protection Act 1998 as the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.

15.3.4 If information is to be processed in this way, individuals must be given the opportunity to opt out from being sent direct marketing or advertising material.

## **15.4 Rights in Relation to Automated Decision Making**

- 15.4.1 An individual is entitled, by written notice, to require an organisation to ensure that no decision that significantly affects them is based solely on the automatic processing of their information. Examples of this are evaluating work performance or reliability or conduct of individuals where no human intervention takes place and decisions are made automatically.
- 15.4.2 Signatories to individual second level protocols must agree procedures as to how this right will be managed.
- 15.4.3 Where an organisation intends to implement such a system, they must inform the individuals concerned of the logic involved and how decisions are made about them, ensuring that some form of human intervention takes place.

## **15.5 Right to Compensation**

- 15.5.1 Individuals have the right to seek compensation via the courts if they suffer damage and distress as a result of any contravention of the requirements of the Data Protection Act 1998 if the organisation cannot prove that they have taken reasonable care in the circumstances to comply with the Data Protection Act 1998.

## **15.6 Requests for Assessment**

- 15.6.1 An individual may ask the Information Commissioner to assess whether or not it is likely that any processing of information has been or is carried out in compliance with the Act. This may lead to enforcement action if it is pursuant to a complaint against the organisation.

## **16.0 Breaches of the Protocol**

- 16.1 Breaches of this protocol will be seen as a matter of serious concern and partner organisations will take immediate action including the possibility of disciplinary action should this be necessary. Breaches of the protocol should be recorded, investigated and findings noted and actioned by the respective officers.

# **LEVEL III: TEMPLATE - STEPS TOWARDS A PROTOCOL**

## **Protocol Management Procedures: Table of Contents**

17.0 Protocol Management Procedures

18.0 Protocol Agreement

19.0 Certification

20.0 Level Three Protocol Requirements

## **17.0 PROTOCOL MANAGEMENT PROCEDURES**

### **17.1 Structures and Responsibilities**

The organisations which are party to a protocol have responsibility for:

- Ownership
- Approving new parties to the protocol
- Approving the content of protocols
- Recommending adoption
- Ensuring dissemination
- Agreeing training programme
- Implementation within organisations
- Monitoring implementation/compliance
- Formal review
- Commissioning work to develop and amend protocol
- Ensuring amendments

17.1.1 It is the responsibility of the Chief Officers/Boards of each organisation to nominate a senior staff member to be responsible for information handling issues within their own organisation, which will involve the development, improvement and review of the protocol.

17.1.2 It should be made clear to staff what steps they need to follow to settle a dispute between organisations on whether information should be shared and who to contact in these circumstances. This should be a named senior staff member. Where the sensitivity of the information requires that staff in one organisation must go through a vetting process (for example CRB or enhanced CRB checks) where vetting is justified, staff from other organisations that have access to the information should be subject to the same vetting procedures. Appropriate checks to ensure the required vetting processes have taken place must be evidenced and documented prior to information sharing taking place.

### **17.2 Formal Approval and Adoption**

17.2.1 Responsibility for the adoption, approval, maintenance and review of these protocols will be assigned to an appropriate senior level steering group. It is the responsibility of the Chief Officers/ Boards of each organisation to nominate a senior member of staff to be a member of this group and ensure the responsibilities at 17.1, 17.1.1 and 17.1.2 are undertaken within their own organisation.

17.2.2 Protocols will apply to the organisations listed within the protocol and to all staff including, students, agency workers, sub-contractors, volunteers and seconded staff working within those organisations.

### **17.3. Dissemination/Circulation of Protocol**

- 17.3.1. Protocols will be introduced to managers and staff (students, employees, agency staff, volunteers and seconded staff) through a programme of multi-agency briefings and training events that will take place at least one month before any protocol becomes effective. Staff within organisations responsible for sub contractors will ensure that sub contractors are aware of their responsibilities within any protocol.
- 17.3.2. Copies of protocols will be circulated to all relevant staff, in line with each organisation's internal arrangement for distribution of procedures and guidelines. Wherever possible, the protocol will also be available to staff on-line, on the organisations intranets and websites.
- 17.3.3. The content of the protocols will be where appropriate communicated to individuals and where relevant to carers and voluntary organisations to ensure that individual rights in relation to the disclosure and use of personal information are understood and upheld.
- 17.3.4. A strategy for disseminating protocols to the public will be developed in line with the need to ensure that members of the public are fully informed about their rights in relation to disclosure of personal information.
- 17.3.5. Protocols will be published on the web-sites of the organisations involved and made available at key information points. Each of the partner organisations will keep sufficient copies to enable relevant protocols to be readily available to members of the public who require them.
- 17.3.6. Plans for disseminating a protocol to the public will be finalised no later than one month before the date on which the protocol is to become effective.

### **17.4 Reviewing the Protocol**

- 17.4.1. The protocol will be subject to a regular formal review process instigated and managed by a designated individual.
- 17.4.2. Following consultation with the individual(s) nominated at 17.1.1 agreed changes will be forwarded to the Chief Officers/Boards for formal approval and adoption.
- 17.4.3. Staff will be informed of all changes to the protocol, training will take place if the changes are substantial and all documentation in paper and electronic format will be appropriately amended when the changes become effective. If changes are very substantial where for example operational problems and complaints have arisen on a

regular basis the protocol should be completely rewritten and implemented with the necessary training for staff.

## **17.5 Monitoring the Protocol**

- 17.5.1 The individual nominated at 17.1.1 will be responsible for monitoring compliance with the protocol.
- 17.5.2 Instances of internal non-compliance will be logged and dealt with promptly. Non-compliance by a partner organisation will be reported to that organisation's individual nominated at 17.1.1 and the review process defined in 17.4.- 17.4.3 above.
- 17.5.3 The following incidents relating to organisations party to the protocol will be logged and reported to the individual nominated at 17.1.1
- Delays in responding to requests for information
  - Disclosure or access to information to members of staff who do not have a legitimate "need to know"
  - Disclosure or access to information to members of staff who have not been appropriately vetted
  - Inappropriate or inadequate use of the procedures
  - Disregard of the procedures, including refusal to disclose information and placing conditions on disclosure that may not be warranted.
  - Use or disclosure of personal data for purposes other than those stated for the organisation

## **17.6 Reporting Breaches, Improvements and Weaknesses of the Protocol**

- 17.6.1 The individual identified in 17.1.1 will investigate all breaches, improvements and weaknesses of the Protocol and report their findings to the Chief Officers/Boards.
- 17.6.2 Any complaint received from, or on behalf of, an individual containing allegations of inappropriate disclosure of information will be dealt with through the internal complaints procedure of that organisation and any other organisations who participated in the information sharing.
- 17.6.3 All complaints regarding inappropriate disclosure will be reported to the individual identified at 17.1.1 who will inform the Chief Officers/Boards of the outcome of the complaints.

## **18.0 Protocol Agreement**

### **18.1 Undertaking**

- 18.1.1 The parties to the protocol agree that the procedures laid down in the protocol will provide a secure framework for the sharing of information

between their organisations in a manner compliant with their statutory and professional responsibilities.

18.1.2 As such, they undertake to:

- implement and adhere to the procedures and structures set out in the protocol
- ensure that all **Individual Protocols** established between their organisations for the sharing of information relating to a defined population are consistent with the first, second and third level templates for devising information sharing protocols.
- ensure that where these procedures are formally adopted, no restriction will be placed on the sharing of information other than those specified within **Individual Protocols**
- Ensure that staff adhere to the procedures and structures within **Individual Protocols**
- Audit compliance with this protocol within their organisation

## 18.2 Indemnity Agreement

18.2.1 The responsibility for any action arising out of failure to comply with this agreement and/or associated operational instructions is to be shared by all parties to the agreement or all those involved in the sharing of the specific information the subject of the claim unless it is shown that one or more of the parties failed to comply with the agreement and/ or any associated operational instructions, in which case that party or those parties shall indemnify each of the other parties against all actions, claims and demands arising from their original or subsequent disclosure.

## 19.0 Certification

19.1.1 All organisations that are party to Individual Protocols must sign the first level protocol . In addition they must sign the relevant level 2 and level 3 protocols.

19.1.2 By signing an **Individual Protocol**, the participants accept and adopt the statements included in it and the indemnity and agree to maintain the specified standards.

19.1.3 In addition the partners to an **Individual Protocol** will not use, release or otherwise disclose any data whatsoever to any organisation which is not a signatory to it, unless it is with the agreement of all signatories or it is necessary for a statutory duty.

## 20.0 Each third level protocol needs to consider

- What information is being shared?
- Who will have access to the information and what may they use it for?

- How will the information being shared be kept accurate and up to date?
- How long a period will the information be retained for?
- How will the information being shared be recorded?
- How is the security of the information being shared ensured?
- Who is accountable for the Information Sharing Protocol (ISP) ?
- Who will approve and authorise the ISP?
- How will organisations ensure compliance with the Data Protection Act 1998 if the information being shared is personal or sensitive personal information?
- Where will the ISP be held?

**And will need to include the following:**

- Any additional definitions and a glossary of terms not provided at Annex A
- any other legislation and guidance not already included in the legal framework provided at Annex A
- Implementation plans, including agreed training provision, for developing, implementing and reviewing and monitoring the protocol
- Any referral assessment, care planning and service provision requirements including a process chart detailing this and consent requirements
- Indemnity agreements
- The development of a leaflet to accompany the consent form including advice to individuals about issues relating to consent and their rights in relation to their information