



ISLINGTON

# Islington Information Sharing Protocol

Version 1.2



# CONTENTS

INTRODUCTION .....	4
1 BACKGROUND .....	4
2 PURPOSE.....	5
3 STATUS AND SCOPE.....	7
4 PARTIES TO THE PROTOCOL.....	8
GOVERNANCE AND REVIEW.....	9
5 PROTOCOLS AT TWO LEVELS.....	11
6 THE GENERAL INFORMATION SHARING PROTOCOL .....	11
7 THE INDIVIDUAL INFORMATION SHARING AGREEMENTS .....	12
LEGAL AND PROFESSIONAL FRAMEWORK .....	14
8 LEGAL BASIS FOR SHARING INFORMATION .....	14
9 KEY PRINCIPLES FOR INFORMATION SHARING .....	16
OBLIGATIONS OF THE PARTIES .....	19
10 GENERAL UNDERTAKINGS BY EACH AGENCY.....	19
11 CONSENT.....	22
12 DISCLOSURE .....	23
13 STORAGE.....	24
14 STAFF AWARENESS AND TRAINING.....	25
FORMAL AGREEMENT .....	26
15 PURPOSES FOR WHICH INFORMATION WILL BE SHARED.....	26
16 AGREEMENT.....	27
17 SIGNATORIES .....	29
APPENDICES.....	34
18 APPENDIX A - LEGISLATION .....	34
19 APPENDIX B - CHECKLIST OF LEGAL CONSIDERATIONS .....	44
20 APPENDIX C - CONSENT: GUIDANCE NOTES.....	46
21 APPENDIX D - PROTOCOL MANAGEMENT PROCEDURES.....	52
TEMPLATES.....	55
22 INDIVIDUAL INFORMATION SHARING AGREEMENT: TEMPLATE.....	55

## DOCUMENT HISTORY

This document has been distributed to:

Version	Date	Author	Released to	Comments
1	Aug 2006	Peter Fehler / Jeremy Tuck	Corporate Management Board	
1	Oct 2006	Jeremy Tuck	Islington Strategic Partnership members and other partners.	

This document requires the following approvals

Date	Version	Name	Role
August 2006	1	Louise Round	Chair of the Information Governance Board
September 2006	1	All members	Corporate Management Board
September 2006	1	All members	Islington Strategic Partnership
October 2006	1.1	All partners	All partners to approve the protocol through their own processes
April 2007	1.2	Signatories added	Signatories added to Section 4 and Section 17

### Copyright Notification

This document is distributed under the Creative Commons Attribution 2.5 license. This means you are free to copy, use and modify all or part of its contents for any purpose as long as you give clear credit for the original creators of the content so used. For more information please see: <http://creativecommons.org/licenses/by/2.5/>

Copyright © London Borough of Islington 2006

# INTRODUCTION

## 1 Background

### 1.1 The need to share information between Islington's partner agencies

- 1.1.1 While the public rightly expect that personal information held by Islington's statutory agencies will be properly protected, there is also a growing expectation that information will be shared in partnership where it is appropriate to do so.
- 1.1.2 Sometimes it is only when information held by different agencies is pulled together that a person is seen to be in need of additional or alternative services. Sharing information, therefore, is a key element to the delivery of high quality, cost effective and seamless public services.
- 1.1.3 In the past there have been both real and perceived barriers to the sharing of personal information. The Data Protection Act 1998 places an emphasis on protecting privacy which has, in the past, made agencies very reluctant to share information for fear of breaking the law. It also, however, meant that information which should have been shared was kept within one agency. There is a need to share information within the framework of clear understanding between agencies.

### 1.2 The need for an Information Sharing Protocol

- 1.2.1 In the absence of specific statutory instruments enabling the sharing of personal information to take place, it is necessary that all partners concerned have a clearly defined framework to facilitate the sharing of personal information whilst respecting the rights of the individual.
- 1.2.2 The objective of the Information Sharing Protocol is to provide a framework of trust between professionals for people who use public services in Islington around the way personal and other information is shared. This is essential to enable public sector agencies to meet both their statutory obligations and the needs and expectations of the people who they serve.
- 1.2.3 It is intended to assist both professionals and the public to feel confident that personal information is being shared in the right ways for the right reasons.
- 1.2.4 The purpose is help agencies to work closer together, and provide the standards of service expected by both government and the public.

## **2 Purpose**

### **2.1 Overarching objectives**

- 2.1.1 To provide a robust framework for the legal, secure and confidential sharing of personal information between public sector partner agencies to enable them to meet both their statutory obligations and the needs and expectations of the people who they serve.
- 2.1.2 The strategic purpose of this General Protocol for the sharing of personal information are:
- a) the delivery of integrated public sector services in line with government initiatives and public expectations,
  - b) to facilitate the management and planning of cost effective and efficient services; and,
  - c) to enable parties to the General Protocol to review, account for, and learn how to improve what they do.
- 2.1.3 The Protocol is an over-arching framework for sharing information between partner Agencies in Islington. It focuses on requirements for sharing personal information about service users.
- 2.1.4 The Protocol:
- a) Clarifies the legal background on information sharing
  - b) Outlines the principles that need to underpin the process
  - c) Provides practical guidance on how to share information in a series of supporting Procedures
  - d) Provides a framework within which organisations can develop Individual Information Sharing Agreements for specific areas of service.
  - e) Includes arrangements for monitoring and reviewing the use of the Protocol and for responding to breaches.
  - f) The Protocol is not contractually binding but is to be used to set good practice standards that the parties need to meet in order to comply with relevant legal duties in relation to the sharing of personal information.

### **2.2 Helping to promote information sharing**

- 2.2.1 The Protocol will help to remove barriers to effective information sharing and will assist in ensuring that service users receive integrated services which is a key principle of Government policy.

### **2.3 Helping to ensure compliance with legislation and guidance**

- 2.3.1 In order to ensure compliance with the 1998 Data Protection Act, organisations must satisfy themselves that the agencies they share information with have proper procedures in place in relation to the way in which they will hold and use that information.

- 2.3.2 The Protocol includes procedural guidance to assist organisations in complying with legislation and guidance and in particular to:
- a) help to ensure that consent to share personal information is obtained from the service user wherever this is necessary
  - b) help ensure that information is shared where there is a requirement to do so
  - c) help ensure that partner organisations have appropriate procedures in place to ensure compliance with legislation
  - d) The Protocol includes detailed procedural guidance on consent issues to assist staff in complying with legal requirements.

## **2.4 Raising awareness**

- 2.4.1 The Protocol raises awareness of the key information sharing issues and provides detailed procedural guidance. Training material will be made available to support implementation. This will help organisations to ensure that staff are aware of these key issues and have confidence in the process of sharing information with others.

### **3 Status and Scope**

#### **3.1 Scope**

- 3.1.1 This Protocol is an agreement between agencies to govern the sharing of personal information about service users and facilitate the development of information sharing agreements. It does not relate to the sharing of personal information about staff.
- 3.1.2 The Protocol focuses primarily on the sharing of “personal” and “sensitive” information about people and also refers to “private” information in relation to the Human Rights Act 1998 and “confidential” information.
- 3.1.3 The Protocol comprises the common principles and procedures to be adopted wherever and whenever these organisations share information for these purposes.

#### **3.2 Status**

- 3.2.1 The Protocol is intended as guidance for staff in the performance of their duties with regard to the sharing of confidential personal information about customers, clients or patients.
- 3.2.2 The Protocol applies to all staff directly employed either by Islington or by other partner organisations: such staff will be instructed that they must not share confidential personal information except in accordance with the protocol. See further Section 10 below in relation to the obligations of individual members of staff.
- 3.2.3 The Protocol is intended to complement any existing professional Codes of Practice that apply to any relevant profession working within either organisation.
- 3.2.4 The Protocol does not constitute legal advice.

## **4 Parties to the protocol**

- a) London Borough of Islington
- b) Islington Primary Care Trust
- c) Metropolitan Police
- d) City & Islington College
- e) Family Mosaic
- f) Factory Community Centre
- g) Islington Law Centre
- h) London Metropolitan University
- i) Homes for Islington
- j) Bolt Burdon Solicitors
- k) James Selby Ltd
- l) Disability Action Islington
- m) Islington Childcare Trust
- n) Tollington Community Association
- o) London Fire Brigade
- p) Job Centre Plus
- q) Holloway Prison
- r) Islington Society
- s) Whittington Hospital
- t) British Association of Settlements and Social Actions Centres
- u) EC1 New Deal for Communities
- v) Finfuture

## GOVERNANCE AND REVIEW

### 4.1 Islington Strategic Partnership

4.1.1 This Information Sharing Protocol will be governed under the Islington Strategic Partnership, which brings together the main local organisations in the borough to help make Islington a better place for everyone. As well as Islington Council and Islington Primary Care Trust, membership in the Islington Strategic Partnership includes the Metropolitan Police plus representatives from education, social housing, business sector, voluntary sector, faiths and the community as a whole.

### 4.2 Formal approval, adoption and review

4.2.1 The General Protocol will be formally signed off by the Islington Strategic Partnership Board. Partner agencies may also need to sign off the protocol internally in line with their own procedures.

4.2.2 Individual Protocols will be signed off by Senior Officers in the agencies concerned.

4.2.3 Formal adoption will follow the signing of the document by the head of each partner agency.

4.2.4 This General Protocol will be managed according to the Protocol Management Procedures, set out in [APPENDIX D - Protocol Management Procedures](#).

4.2.5 The General Protocol will initially be reviewed on an annual basis by the Islington Strategic Partnership Board, who will determine body or individual(s) who will co-ordinate the review.

### 4.3 Local Area Agreements

4.3.1 Local Area Agreements (LAAs) are an agreement between central Government and local strategic partnerships (i.e. the Islington Strategic Partnership) to deliver a set of agreed outcomes and targets over a three to five year period. Central to an LAA is the belief that positive change in a community is best achieved by different sectors working together. LAAs, therefore, represent a new and exciting opportunity for people from the statutory, voluntary and community, business and faith sectors to come together and use their collective, expertise, effort and resources to address the issues that matter most for the people of Islington.

4.3.2 This Information Sharing Protocol needs to serve as a key tool to support work being undertaken as part of the Local Area Agreement.

### 4.4 Islington Children's Board

4.4.1 The Islington Children's Board (ICB) oversees and monitors whether organisations and services are making a difference to support children and young people grow up in Islington and agrees how to improve that support. The ICB meets at least 3 times a year. ICB members include representatives from the council, the Primary Care Trust (PCT), CEA@Islington, the community and voluntary sectors and of other organisations such as Homes for Islington and the Police. Chief officers from the council and the PCT attend as advisers.

4.4.2 The membership of the Board will reflect the partnership between the Council and the Primary Care Trust (PCT). It may, in time, have delegated authority over aspects of the service, as agreed by both partners.

4.4.3 This Information Sharing Protocol will be used as a key tool to support partner agencies of Islington Children's Board and in this context, specifically for information sharing between the council and the Primary Care Trust.

#### **4.5 Safer Islington Partnership**

4.5.1 The Safer Islington Partnership (SIP) is an amalgamation of the Islington crime Reduction Partnership, the Islington Drugs & Alcohol Action Team and the Youth Offending Team. The SIP brings together greater co-ordination of the work formally covered by each partnership to ensure improved strategic planning in the responses to crime and drugs and youth people's involvement in them.

4.5.2 The SIP is made up of lead officers of senior executive level, especially those representing the Lead Authorities, according to the Crime & Disorder Act (1998) and the Police Reform Act (2002). Other partners will be invited to participate in meetings as required and may be involved in discussions and decision-making as appropriate

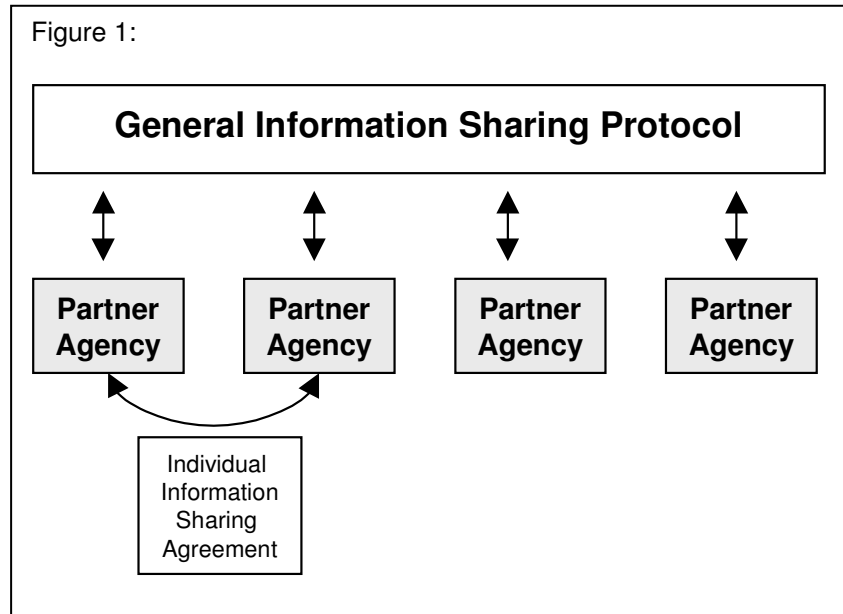
4.5.3 This Information Sharing Protocol will be used as a key tool to support partner agencies of the Safer Islington Partnership.

## 5 Protocols at two levels

### 5.1 Overview

5.1.1 The General Information Sharing Protocol (i.e. this document) provides the legal framework, common principles and procedures for the sharing of personally identifiable information between agencies. It will be supplemented and activated by Individual Information Sharing Agreements for specific areas of service between partner agencies (as indicated in Figure 1) that have signed the agreement.

5.1.2 Each Individual Information Sharing Agreement will set out the detailed arrangements relevant to that particular application. All Individual Information Sharing Agreements will need to be fully compliant and consistent with this Protocol.



## 6 The General Information Sharing Protocol

6.1.1 Clarifies the legal background on information sharing

6.1.2 Outlines the principles that need to underpin the process

6.1.3 Provides a framework within which organisations can develop Individual Information Sharing Agreements (IISAs) for specific areas of service

6.1.4 Includes arrangements for monitoring and reviewing the use of the Protocol and for responding to breaches.

6.1.5 The Protocol is not contractually binding but is to be used to set good practice standards that the parties need to meet in order to comply with relevant legal duties in relation to the sharing of personal information.

## 7 The Individual Information Sharing Agreements

### 7.1 Template

7.1.1 A blank template Individual Information Sharing Agreement is provided in the Templates section (see the [Individual Information Sharing Agreement: Template](#))

### 7.2 Working within the General Protocol

7.2.1 The Individual Information Sharing Arrangement will specifically make reference to the overarching agreement and state that it is working within the framework of the overarching agreement.

### 7.3 Process for preparing an individual agreement

7.3.1 A specific process needs to be undertaken each time an Individual Information Sharing Agreement is set up. This is made up of a series of steps.

### 7.4 Proposal

7.4.1 The proposal should define the key points of the agreement and provide a management summary of the requirement. It should identify the legal, security and procedural issues for the proposed arrangements.

### 7.5 Single point of contact

7.5.1 There needs to be a designated officer in each of the partner agencies who will serve as the single point of contact for the Individual Information Sharing Agreement. This person will be responsible for day-to-day arrangements. In particular, this officer is responsible for:

- a) controlling the release of the information
- b) the integrity of the information (that everything that needs to be disclosed is disclosed)
- c) ensuring that the information is received by an authorised individuals or groups
- d) maintaining a record of disclosures

### 7.6 Sponsorship

7.6.1 The Sponsor will own the relationship with the partner agency specified in the Individual Information Sharing Agreement and will therefore need to be sufficiently senior to take this responsibility. This Sponsor must validate the arguments in the Individual Information Sharing Agreement. In addition, the Sponsor must provide adequate resources for both the production of the agreement and implementation of the arrangements.

7.6.2 The Sponsor needs to ensure that they have permission to share the information from the "owner" of the information. The information owner is a member of staff

Figure 2: Process for preparing an Individual Information Sharing Agreement:



who owns the business area most closely associated with the system from which the information is extracted.

## **7.7 Legal Basis**

7.7.1 The agreement must clearly indicate the sound legal basis for the proposed arrangements. This may be a statutory requirement or a statement of operational necessity.

## **7.8 Security Risk Assessment**

7.8.1 A security risk assessment needs to be undertaken. Both partners will need to work closely to agree specific handling measures of the information. The risk assessment will need to include:

- a) an evaluation and statement around the nature of the information
- b) detail how the information will be transferred
- c) detail safeguards to protect the information during transit
- d) detail safeguards for how this information will be held
- e) highlight any risks and what can be done to mitigate these risks

## **7.9 Individual Information Sharing Agreement prepared and signed**

7.9.1 The Individual Information Sharing Agreement must describe:

- a) the process that was undertaken to prepare the agreement.
- b) procedures for an annual review

## **7.10 Storing the Information Sharing Agreement**

7.10.1 Final original copies of the agreement need to be stored appropriately. This means there should be sufficient controls in place to be able to prevent unauthorised access, destruction, alteration or removal.

## LEGAL AND PROFESSIONAL FRAMEWORK

### 8 Legal Basis for Sharing Information

#### 8.1 Understanding the legal framework for information sharing

- 8.1.1 The legal framework within which public sector data sharing takes place is complex and overlapping and there is no single source of law that regulates public sector information sharing (see [APPENDIX A - Legislation](#)).
- 8.1.2 It is essential that practitioners sharing information are clearly aware of the legislative framework within which they are operating.
- 8.1.3 The purpose, therefore, of detailing the law within this protocol is to highlight the legislative framework, rather than to serve as a definitive legal reference point.

#### 8.2 How to approach questions around information sharing

- 8.2.1 In order to approach questions around information sharing the protocol contains [APPENDIX B - Checklist of legal considerations](#) which raises some of the questions in a more user-friendly way.
- 8.2.2 In summary this comes down to:
- a) Establish whether there is power to carry out the function to which the information sharing relates.
  - b) Check whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of other statutory, common law or other provisions.
  - c) Decide whether the sharing of the data would interfere with rights under Article 8 of the European Convention on Human Rights in a way which would be disproportionate to the achievement of a legitimate aim and unnecessary in a democratic society.
  - d) Decide whether the sharing of the data would breach any obligations of confidence.
  - e) Decide whether the data sharing would be in accordance with the Data Protection Act 1998, in particular the Data Protection Principles.

#### 8.3 Legislation and guidance

- 8.3.1 The collection, use and disclosure of personal information is governed by a number of different areas of law and this Protocol has been drawn up taking these into account. These are detailed in [APPENDIX A - Legislation](#).
- a) The Human Rights Act 1998 and the European Convention on Human Rights
  - b) The Data Protection Act 1998
  - c) The law that governs the actions of public bodies (administrative law)
  - d) The common law tort of breach of confidence
  - e) European Union law.
  - f) Access to Health Records Act 1990
  - g) Crime and Disorder Act 1998

- h) Common Law Duty of Confidentiality
- i) Local codes or standards relating to confidentiality
- j) Caldicott guidelines
- k) Freedom of Information Act 2000
- l) Regulation of Investigatory Powers Act 2000

#### **8.4 Inter-authority Freedom of Information Act (FOIA) 2000 requests**

- 8.4.1 From time to time, a request may be made under FOIA for information that has been shared under this protocol. These “inter-authority requests” are to be handled in accordance with the procedures set out below. The authority that receives the FOIA request (the “receiving authority”) is responsible for answering the request. In doing so the receiving authority must comply with the procedural requirements of FOIA (for instance, the requirement to identify any exemptions relied upon, and where necessary to explain the basis on which those exemptions are thought to apply).
- 8.4.2 The receiving authority, and the authority that disclosed to the receiving authority the information that is sought in the request, must seek if at all possible to agree whether the information is to be disclosed: the fullest consideration will be given to either authority’s claim that an exemption applies. If there is a dispute between two agencies as to whether or not information should be disclosed, then the receiving agency is guided to consider the option of non-disclosure of the information. This will enable the applicant, if not satisfied with the outcome, to proceed to a complaint stage where the decision-making process can be reviewed by the receiving agencies’ internal complaint process.
- 8.4.3 The legal obligation is clear – an agency receiving a request for information that it holds has a duty to disclose that information unless an exemption applies – this ensures that inter-agency requests are dealt with in a manner that will provide the best service to the applicant and ensure that decisions on the disclosure or non-disclosure of information are dealt with in a co-ordinated approach.
- 8.4.4 The Code under s.45 FOIA outlines further responsibilities on a public body to transfer requests for information that it does not hold, where it is believed to be held by another organisation. The public body will consider whether to:
  - a) consult the other organisation with a view to establishing whether information is held
  - b) transfer the request, either in full or the part of the request that relates to information held elsewhere, with the consent of both the applicant and the other agency
- 8.4.5 The receiving agency must still advise the applicant that it does not hold the information (or part of it), consider the appropriateness of advising the applicant that the information is held elsewhere and seek the applicant’s consent to transfer the request. Information held by the receiving agency that can be disclosed must be so disclosed whilst the remainder of the request is transferred. The FOIA officer within each organisation is responsible for this process.

## **9 Key principles for information sharing**

9.1.1 A number of safeguards are necessary in order to ensure a balance between maintaining confidentiality and sharing information appropriately.

9.1.2 The sharing of information by organisations under the Protocol will be based on the following principles:

### **9.2 Commitment to sharing information**

9.2.1 Partner organisations recognise that multi-agency initiatives require a commitment to sharing personal information about service users in compliance with guidance and legislation.

### **9.3 Statutory duties**

9.3.1 Partner organisations are fully committed to ensuring that they share information in accordance with their statutory duties including the requirements of the Data Protection Act 1998 and the Human Rights Act 1998.

### **9.4 Caldicott requirements**

9.4.1 All organisations recognise the requirements that Caldicott imposes on NHS organisations and Social Services Departments. They will ensure that requests for information from these organisations are dealt with in a manner compatible with these requirements.

### **9.5 Duty of confidentiality**

9.5.1 All organisations which are party to this protocol recognise the importance of the legal duty of confidentiality, and will not disclose information to which this duty applies without the consent of the person concerned, unless there are statutory grounds and an overriding justification for so doing. In requesting release and disclosure of information from partner organisations, all staff will respect this responsibility.

### **9.6 Consent**

9.6.1 Wherever possible organisations will seek consent from the service user to share personal information. Where consent to disclose information is requested, the service user will be made fully aware of the information it is proposed to share and the purposes for which it will be used. If a person is unwilling to give consent, information will only be shared in exceptional circumstances and where there are appropriate statutory grounds for doing so.

### **9.7 Sharing without consent**

9.7.1 Organisations will put procedures in place to ensure that decisions to share

personal information without consent have been fully considered and comply with the requirements of the relevant legislation. Such decisions will be appropriately recorded for audit purposes. All relevant staff will be provided with training in these procedures.

## **9.8 “Need to know”**

9.8.1 Where it is agreed necessary for information to be shared, this will be done on a “need-to-know” basis only i.e. the minimum information consistent with the purpose for sharing will be given.

## **9.9 Information kept confidential from the service user**

9.9.1 Where an organisation believes that information supplied by them should be kept confidential from a service user, the outcome of this request and the reasons for taking the decision will be recorded. Such decisions will only be taken on statutory grounds.

## **9.10 Specific purpose**

9.10.1 Partners will not abuse information that is disclosed to them under the specific purposes set out in the protocol. 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.

## **9.11 Fact / opinion**

9.11.1 When disclosing information about an individual, professionals will clearly state whether the information being supplied is fact, opinion, or a combination of the two.

## **9.12 Use of anonymised information where possible**

9.12.1 Personal information will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is necessary. For all other purposes, information about individual cases will be anonymised.

## **9.13 Access to information**

9.13.1 People will be fully informed about the information that is recorded about them. They will be able to gain access to information held about them and to correct any factual errors that may have been made. If an organisation has statutory grounds for restricting a person's access to information about them, they will be told that such information is held and the grounds on which it is restricted. Where opinion about a service user is recorded and they feel the opinion is based on incorrect factual information, they will be given the opportunity to correct the factual error and record their disagreement with the recorded opinion.

## **9.14 Complaints procedures**

9.14.1 Partners are committed to having procedures in place to address complaints

relating to the disclosure of information. Service users will be provided with information about these procedures.

**9.15 Staff awareness**

9.15.1 Partner organisations will ensure that all relevant staff are aware of and comply with their responsibilities in relation to:

- a) the Protocol
- b) the confidentiality of information about service users
- c) the commitment to share information in accordance with guidance and legislation

**9.16 Disciplinary action**

9.16.1 Partner organisations will ensure that contracts of employment and standing orders include reference to the issue of disciplinary action should staff disclose personal information on a basis which cannot be justified on statutory grounds.

## OBLIGATIONS OF THE PARTIES

### **10 General undertakings by each agency**

#### **10.1 To nominate a lead person**

- 10.1.1 Agencies who are party to the General Protocol will nominate a lead person who will be responsible for the day-to-day management of the scheme within their agency and the approval of this protocol and any Individual Information Sharing Agreements.
- 10.1.2 The person nominated as 'Lead Person' should have sufficient seniority within the agency to influence policies and procedures at executive level.
- 10.1.3 It is anticipated that within NHS or Social Care agencies this person will be the Caldicott Guardian.

#### **10.2 To ensure minimum standards for all Individual Sharing Agreements**

- 10.2.1 In order to maintain a consistent approach, all agencies who are party to the General Protocol will ensure that any Individual Information Sharing Agreements contains the following information:-
  - a) The full details of the agencies who are party to the agreement (e.g. names and addresses).
  - b) The purpose(s) for the sharing of personal information.
  - c) The type(s) of personal information that will be shared.
  - d) Details of any other agencies/organisation to whom the personal information may also be shared by the recipient.
  - e) Details of any restrictions on the use of the personal information.
- 10.2.2 All Individual Protocols will be approved by the respective lead person nominated within each agency.
- 10.2.3 A specimen Individual Protocol is provided in the Templates section at the end of this document, see [Individual Information Sharing Agreement: Template](#).
- 10.2.4 Where information sharing protocols exist between agencies prior to signing up to the General Protocol, such protocol will remain valid. However, such protocols should be reviewed and if necessary brought into line with the General Protocol at the earliest opportunity in order to maintain a consistent approach.

#### **10.3 To comply with a duty of confidentiality**

- 10.3.1 Personal information held by an agency shall be deemed to have been provided in confidence, in the absence of explicit or implied confirmation, when it appears reasonable to assume that the provider of the information believed that this would be the case.
- 10.3.2 All agencies who are party to the General Protocol accept this duty of confidentiality and will not disclose personal information without the consent of the person concerned, unless there are statutory grounds or other overriding

justification for so doing.

- 10.3.3 In requesting disclosure of personal information from another agencies who is party to the General Protocol, those concerned will respect this responsibility and not seek to override the procedures which each agencies has in place to ensure that information is not disclosed illegally or inappropriately.

#### **10.4 To comply with legislation**

- 10.4.1 Agencies who are party to this General Protocol recognise their responsibilities with regard to legislation and the use of personal information which they have acquired and shall have in place appropriate policies and procedure to ensure that personal information within their care is used within the context of the relevant legislation, in particular the Data Protection Act 1998.
- 10.4.2 Agencies party to the General Protocol recognise the sensitivity of information about a person's racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical and mental health, sexuality, the commission or alleged commission of any offence and any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings and will adhere to the requirements of Schedule 3 of the Data Protection Act 1998 in respect of such information.
- 10.4.3 Agencies who have obtained information in any of the above mentioned categories about an individual, in the course of their direct contact with that person, will seek to obtain the explicit consent of that person to disclose that information to another agency. If consent is not given, because the person is either unable or unwilling to give that consent, then the information will only be released if there are legal grounds for doing so and one of the remaining conditions of Schedule 3 can be demonstrated or there is a statutory reason for doing so without the individual's consent.

#### **10.5 To deal with requests for access to partner records in the way set out below**

- 10.5.1 A service user making a valid request under section 7 of the Data Protection Act 1998 for access to his/her record will be fully informed, in accordance with the Act, about the information that is held about them by the agency approached.
- 10.5.2 Information that has been provided by another agency under an agreed Individual Information Sharing Agreement may be disclosed to the individual without the need for obtaining the provider's consent to disclose, with the following exceptions when consent must be obtained prior to disclosure:-
- a) The provider has specifically stated that the information supplied must be kept confidential from the service user.
  - b) The information contains medical details.
  - c) The information contains information of a legal nature.
- 10.5.3 In the situation of two or more organisations having a joint (single) record on an individual, that individual may make their access to record request to any of the

organisations. The organisation receiving the request will be responsible for processing the request for the whole record and not just the part that they may have contributed, subject to the conditions for disclosure mentioned above.

## **10.6 To put in place a Complaints Procedure relating to disclosure of information**

- 10.6.1 Agencies who are party to this General Protocol shall put in place efficient and effective procedures to address complaints relating to the disclosure or the use of personal information that has been provided under an agreed Individual Protocol.
- 10.6.2 In the event of an complaint relating to the disclosure or the use of an individual's personal information that has been supplied/obtained under an agreed Individual Protocol, all agencies who are party to the Individual Protocol will provide co-operation and assistance in order to resolve the complaint.
- 10.6.3 All agencies will ensure that the service users will be provided with information about the complaints procedures when consent is obtained or upon request.

## **10.7 To put in place measures to address compromises of Confidentiality**

- 10.7.1 All agencies who are party to the General Protocol will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal information whether intentional or inadvertent.
- 10.7.2 In the event of personal information that has been shared under the General Protocol having or may have been compromised, whether accidental or intentional, the agency making the discovery will without delay:-
  - a) Inform the information provider of the details.
  - b) Take steps to investigate the cause.
  - c) If appropriate, take disciplinary action against the person(s) responsible.
  - d) Take appropriate steps to avoid a repetition.
- 10.7.3 On being notified that an individual's personal information has / have been compromised, the original provider will assess the potential implications for the individual whose information has been compromised and if necessary:-
  - a) notify the individual concerned,
  - b) advise the individual of their rights,
  - c) provide the individual with appropriate support.

## **10.8 To comply with the following in wanting to use Personal Information other than for an agreed purpose**

- 10.8.1 It is recognised that agencies who are party to the General Protocol may fulfil a number of roles. In fulfilling one particular role, they may be given privileged access to personal information which they may subsequently believe may assist them in another role or be of wider interest to their organisation.
- 10.8.2 Personal information shared under this General Protocol will have been disclosed for a specific purpose, as defined in the Individual Protocol, and as such must only be used for that purpose.

- 10.8.3 Personal information that has been obtained under an agreed Individual Protocol will not be regarded or used by the receiving agency as intelligence for the general use of that organisation.
- 10.8.4 Agencies wishing to use information given under the General Protocol for any purpose other than that defined in the Individual Protocol, or who may wish to disclose that information to any person other than those authorised to receive that information, must:-
  - a) inform the originator of the information of their intention to use the information provided for a different purpose, and
  - b) Obtain explicit consent from the individual(s) concerned before processing such information.
- 10.8.5 Agencies who wish to use information that has been provided to them under the General Protocol for research or statistical purposes must ensure that policies and procedures are in place to guarantee that such personal information is anonymised.

## **11 Consent**

### **11.1 To seek informed explicit consent**

- 11.1.1 Unless statutory exemptions are applicable, all agencies who are party to the General Protocol will endeavour to seek informed explicit consent from the individual concerned to share their personal information in accordance with an agreed Individual Protocol.
- 11.1.2 Consent will normally be obtained at the earliest opportunity and should be sufficient to cover the needs for a particular 'piece of work' or situation. It is essential to avoid the need to repeatedly seek consent over minor issues.
- 11.1.3 In seeking consent to disclose personal information, the individual concerned will be made fully aware of the nature of the information that it may be necessary to share, who the information may be shared with, the purposes for which the information will be used and any other relevant details including their right to withhold or withdraw consent.
- 11.1.4 For further guidance on consent, see [APPENDIX C - Consent: Guidance notes](#).

### **11.2 To observe and comply with a Time Limit On Consent as set out below**

- 11.2.1 Consent to disclose personal information, obtained under an Individual Protocol, will be limited to the duration of the 'piece of work'.
- 11.2.2 All agencies participating in the General Protocol agree that once the 'piece of work' for which consent was originally obtained has been completed, that consent will be deemed to have lapsed.
- 11.2.3 In the event that a similar, or subsequent additional work needs to be undertaken with that individual, a new consent to disclose will be obtained.

### **11.3 To record obtaining consent in the way set out below**

- 11.3.1 The agency obtaining explicit consent to disclose an individual's personal information will retain the signed original consent form on the individual's manual record.
- 11.3.2 The agency obtaining explicit consent to disclose an individual's personal information will provide the person giving consent with a copy.
- 11.3.3 The agency obtaining explicit consent to disclose an individual's personal information will provide a copy of the consent form to the other agency/agencies involved when the initial disclosure is made.
- 11.3.4 All agencies participating in the General Protocol will ensure that the details (including any conditions) of any consent, or refused consent, are recorded on their electronic systems in accordance with their agencies policies and procedures.

### **11.4 To deal with withdrawal of consent or amend restrictions in the way set below**

- 11.4.1 In the event that an individual (a) Withdraws his/her consent for their personal information to be shared, or (b) Wishes to subsequently place/amend a restriction upon the personal information to that may be shared, the agency receiving such a request will immediately inform all other agencies who are or may be affected and record the details on the individual's file.
- 11.4.2 In the case of consent being withdrawn, no further personal information should be disclosed unless there are statutory reasons for doing so, or a legal exemptions can be applied.
- 11.4.3 In the case of the person applying restrictions on the use of their personal information, these restrictions should be complied with unless there are statutory reasons for doing so, or a legal exemptions can be applied.

## **12 Disclosure**

### **12.1 To address Disclosure Without Consent in the way set out below**

- 12.1.1 Agencies who are party to the General Protocol will put in place procedures to ensure that decisions to disclose personal information without legal grounds or consent have been fully considered and that such a decisions can be audited and defended.
- 12.1.2 A decision to disclose personal information without the consent of the individual concerned should be authorised by a senior member of staff (nominated person) and the reason(s) recorded on the service user's record.
- 12.1.3 On disclosure of the information, the agency providing the information will make the receiving agency aware that disclosure is being made without consent and the reason(s) why.
- 12.1.4 Personal information will only be disclosed where the relevant agreed purpose for sharing clearly requires this. For all other purposes, information about individual cases will be anonymised.

## **12.2 To disclose information in the way set out below**

- 12.2.1 Agencies who are party to the General Protocol will ensure that their staff, who are authorised to make disclosure of personal information, will clearly state whether the information that is being supplied is fact, opinion, or a combination of the two.
- 12.2.2 Unless it is specified to the contrary, all personal information that is provided under an agreed Individual Protocol will be made available to the individual should that individual make a valid request to the recipient for access to their record under section 7 of the Data Protection Act 1998 without the necessity of seeking the providers consent to disclose, subject to the exceptions specified in 10.5.2. It is therefore the responsibility of the person providing the information to clearly state that they do not wish the information to be disclosed without being consulted first.

## **12.3 To record information disclosed under these protocols in the following way**

- 12.3.1 Agencies who are party to the General Protocol will ensure that all personal information that has been disclosed to them under an agreed Individual Protocol will be recorded accurately on the individual's manual or electronic record in accordance with their agencies policies and procedures.
- 12.3.2 Agencies who are party to the General Protocol will set in place procedures to record not only the details of the information, but who gave and who received that information.

## **12.4 To disclose personal information of deceased person(s) as below**

- 12.4.1 Agencies who are party to the General Protocol will exercise caution when contemplating the disclosure of personal information relating to a deceased person. Although the Data Protection Act only applies to personal information of a living person, a duty of confidentiality may still apply after the person has died.

# **13 Storage**

## **13.1 To store personal information securely with set policies and procedures**

- 13.1.1 All agencies who are party to the General Protocol will put in place policies and procedures governing the secure storage of all personal information retained within their manual and/or electronic systems.

## **13.2 To put in place policies and procedures for access**

- 13.2.1 All agencies who are party to the General Protocol will put in place policies and procedures governing the access by their employees, and others, to personal information held within their manual and/or electronic systems and to ensure that access to such information is controlled and restricted to those who have a legitimate need to have access.

## **13.3 To put in place retention and destruction policies and procedures**

- 13.3.1 All agencies who are party to the General Protocol will put in place policies and

procedures governing the retention and destruction of records containing personal information retained within their manual and/or electronic systems.

### **13.4 To put in place policies and procedures for secure transfer**

13.4.1 All agencies who are party to the General Protocol will put in place policies and procedures that govern the secure transfer of personal information both internally and externally. Such policies and procedures must cover:

- a) Internal and external postal arrangements.
- b) Verbally; face-to-face and telephone.
- c) Facsimiles (safe haven).
- d) Electronic mail (secure network or encryption).
- e) Electronic network transfer.

## **14 Staff awareness and training**

### **14.1 To ensure staff under this protocol sign a confidentiality agreement**

14.1.1 All agencies who are party to the General Protocol should require their staff (full/part time; temporary; agency; students etc) who have access to, or are likely to come into contact with, personal information should be required to sign a confidentiality agreement as part of their terms and conditions of employment.

### **14.2 To ensure that staff under this protocol comply to their obligations**

14.2.1 Agencies who are party to the General Protocol will ensure that all staff are aware of, and comply with, their responsibilities and obligations with regard to the confidentiality of personal information about people who are in contact with their agency.

14.2.2 That all staff are aware of, and comply with the commitment of the organisations/agency to only share information legally and within the terms of an agreed Individual Protocol.

14.2.3 That all staff are aware of, and comply with the commitment that information will be shared on a need-to-know basis only.

14.2.4 That staff will be made aware that disclosure of personal information which cannot be justified, whether inadvertent or intentional will be subject to disciplinary action.

### **14.3 To ensure that staff are trained to enable them to share information legally**

14.3.1 All parties to the General Protocol will ensure that employees who need to share personal information under an Individual Protocol are given appropriate training to enable them to share information legally, comply with any professional codes of practice and comply with any local policies and procedures.

14.3.2 Staff who are not directly involved with sharing personal information should not be excluded from such training as it is possible that they may come across such information during the course of their duties. It may therefore be appropriate that such employees receive awareness training.

## FORMAL AGREEMENT

### **15 Purposes for which information will be shared**

15.1.1 Information will only be disclosed where the relevant agreed purpose for sharing clearly requires this. However, each agency must have regard to its legal power in deciding whether they can share information for that particular purpose. The following range of purposes are agreed as justifiable for the transfer of personal information between the Partner Agencies as defined within the remit of this protocol:

- a) assessment of need, service delivery and treatment;
- b) assuring and improving the quality of care and treatment;
- c) monitoring, reporting and protecting public health;
- d) managing and planning future services;
- e) contracting for NHS and other services;
- f) training of staff;
- g) auditing agencies' accounts and performance;
- h) statutory notification of births, deaths and infectious diseases;
- i) medical, health or social care research (subject to ethical approval);
- j) risk management;
- k) statistical analysis;
- l) compliance with court orders;
- m) prevention of crime or disorder;
- n) investigation of complaints or potential legal claims;
- o) medical reports/insurance requests;
- p) drug research/ trials.

### **15.2 Relevant information**

15.2.1 Consideration must be given to the extent of any personal information that is proposed to be disclosed, taking into account the circumstances of the proposed disclosure. It may not be necessary to disclose all information held regarding a service user and only such information as is relevant for the purpose for which it is disclosed should be passed under the sharing arrangement to the recipient(s).

## **16 Agreement**

### **16.1 The undersigned parties agree to:**

- 16.1.1 Promote good practice in the sharing of personal information by ensuring compliance with the principles, purposes and processes of this Protocol
- 16.1.2 Take necessary action to identify and rectify any breaches of the Protocol and to have established policies and practices for dealing with complaints about the sharing of information
- 16.1.3 Facilitate the exchange of information where necessary to promote good quality health and social care and support
- 16.1.4 Ensure that no restrictions are placed on sharing personal information other than those that are specified in this Protocol
- 16.1.5 Ensure that patients and clients are informed of their rights in respect of personal information, including right of access and the complaints procedure
- 16.1.6 Develop systems of implementation, dissemination, guidance, training and monitoring to ensure that the Protocol is known, understood and followed by all professionals who need to share personal information
- 16.1.7 Establish processes to review the use of the Protocol, in order to ensure that practice is in accordance with the requirements of the Protocol, and to take corrective action as needed
- 16.1.8 Develop and amend the Protocol according to any changes to the law or future national guidance
- 16.1.9 Develop information processing systems that ensure collected data is complete, accurate, kept up-to-date and relevant
- 16.1.10 Ensure that collected data is stored and transmitted securely

### **16.2 Indemnity**

- 16.2.1 Disclosure of personal information without consent must be justifiable on statutory grounds, or a meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.
- 16.2.2 Where a disclosing agency provides information to a requesting agency both parties shall assume that both the request and the disclosure are compliant with the requirements of the Data Protection Act 1998.
- 16.2.3 if subsequently it is found that either the request for, or the disclosure of, information is in contravention of the requirements of the Data Protection Act 1998, the agency that originally breached the requirements of the Data Protection Act 1998, either in requesting or disclosing information, shall indemnify the other agency against any liability, cost or expense thereby reasonably incurred, provided that this indemnity shall not apply:
  - a) Where the agency originally found to be in breach of the Data Protection Act 1998 did not know and, acting reasonably had no reason to know, that it had

acted in breach of the Data Protection Act 1998 either in requesting or disclosing information

- b) unless either agency notifies the other agency as soon as reasonably practical of any action, claim or demand against itself to which it considers this indemnity may apply, permits the other agency to deal with the action, claim or demand by settlement or otherwise, and renders all reasonable assistance in doing so.

### **16.3 Agreement**

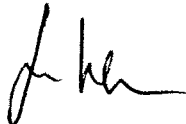

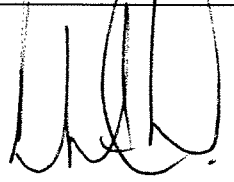

16.3.1 In consideration of the provision of information in accordance with this General Protocol within Islington each person or authority being a Signatory undertakes to indemnify each of the other Signatories against any liability which may be incurred such Signatory as a result of the provision of such information.

16.3.2 Provided that this indemnity shall not apply:-





- a) in the event of the liability arising from information supplied which is incomplete or incorrect and where the error or omission was due to the wilful wrongdoing or negligence of any member or employee of the Signatory providing the information;
- b) unless the Signatory claiming the benefit of this indemnity notifies a Signatory by notice in writing to its Chief Officer providing information or notice as soon as possible of any action claim or demand to which this indemnity applies and permits such Signatory to deal with the action claim or demand by settlement or otherwise and renders to such Signatory all reasonable assistance in so doing.
- c) to the extent that a Signatory claiming the benefit of this indemnity makes any admission which may be prejudicial to the defence of the action claim or demand.

## 17 Signatories

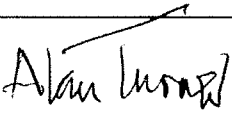
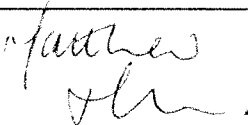
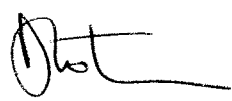
This protocol is signed by the following on behalf of their organisations:

Representing	Name	Signature	Date
London Borough of Islington	Cllr James Kempton (Leader of the Council)		14/5/07
Islington Primary Care Trust	Rachel Tyndall (Chief Executive)		25.04.07
Metropolitan Police	Bob Carr (Borough Commander)		17.05.07
City & Islington College	Frank McLoughlin (Principal)		
Family Mosaic	Brendan Sarsfield (Chief Executive)		
Factory Community Centre	David Vandivier		
Islington Law Centre:	Ruth Hayes		25.07.07

*Please leave blank*

Representing	Name	Signature	Date
London Metropolitan University	Dr Jennifer Somerville (Director)		04/10/07
Homes for Islington	Eamon McGoldrick (Chief Executive)		25/04/07
Bolt Burdon Solicitors	Lynne Burdon		
James Selby Ltd	Wendy Widdecombe		25.04.07
Disability Action Islington	Tracey Lazard		
Islington Childcare Trust	Annie Doubledee		
Tollington Community Association	Theresa Coyle		
London Fire Brigade	Peter Cowup (Borough Fire Commander)		20/11/2007
Job Centre Plus	Michael Hickey		

*Please leave blank*

Representing	Name	Signature	Date
Holloway Prison	Tony Hassall		
Islington Society	Andrew Bosi		25/04/07
Whittington Hospital	David Sloman		
British Association of Settlements and Social Actions Centres	Mark Parker		
EC1 New Deal for Communities	Matthew Humphreys		25/04/07
Finfuture	Despina Johnson		18.5.07

## APPENDICES

### **18 APPENDIX A - Legislation**

#### **18.1 Introduction**

- 18.1.1 Legislation, under which most public sector agencies operate, defines the role, responsibility and power of the agency to enable it to carry out a particular function.
- 18.1.2 In many instances legislation tends to use broad or vague statements when it come to the matter of sharing personal information, for example: the agency is required to communicate., or will co-operate with.. without actually specifying exactly how this may be done. This is because legislation that specifically deals with use of personal information (collection; use; storage; destruction; protection etc.) already exists namely, the Data Protection Act 1998.
- 18.1.3 The Data Protection Act 1998, in most cases, is the key to the use of personal information and links into most other legislation. The Act sets out to govern the collection, use, storage, destruction and protection of a living person's identifiable information (Personal Data). In general, recorded information held by public authorities about identifiable living individuals will be covered by the Data Protection Act 1998. It is important to take account of whether the information is held in paper records or in automated form (such as on computer or on a CCTV system): some of the provisions of the Data Protection Act 1998 do not apply to certain paper records held by public authorities. Broadly speaking, the eight data protection principles set out in Schedule 1 to the Data Protection Act 1998, and discussed further below, will apply to paper records held in a "relevant filing system" or an "accessible record", but not to other paper records.
- 18.1.4 The Data Protection Act 1998 does not set out to prevent the sharing of personal information. To the contrary, providing that the necessary conditions of the Act can be met, sharing is perfectly legal.

#### **18.2 Administrative Law**

- 18.2.1 The principles of administrative law regulate the activities of public bodies; these principles are mainly enforced by way of claims for judicial review in the courts. The courts do not generally review the merits of public law decisions but consider the legality, rationality or procedural propriety of decisions made by public bodies. The rules relating to illegality are most relevant to data sharing: a public body may not act in excess of its powers. If it does act in excess of its powers, then the act is said to be ultra vires. Acts within a public body's powers are said to be intra vires. Under the Human Rights Act 1998, an act of a public authority may be unlawful on the basis that is contrary to the European Convention on Human Rights ("the Convention"). Where questions involving the Convention are involved, the Court will need to consider the merits of the decision more closely than would be the case where the traditional administrative law principles are involved.
- 18.2.2 Local authorities derive their powers entirely from statute and cannot act outside those limited statutory powers. Most of these statutory powers relate to specific local authority functions. In addition to these specific powers, section 111 of the

Local Government Act 1972 provides that local authorities are empowered to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions. Section 2 of the Local Government Act 2000 confers a wide (but not unlimited) power on local authorities to promote the well-being of their area.

- 18.2.3 There is no general statutory power to disclose data, and there is no general power to obtain, hold or process data. As a result, it is necessary to consider the legislation that relates to the policy or service that the data sharing supports. From this, it will be possible to determine whether there are express powers to share data, or whether these can be implied. Express powers to share data are relatively rare and tend to be confined to specific activities and be exercisable only by named bodies. Implied powers will be more commonly invoked. Alternatively it may be possible to rely on section 111 of the 1972 Act or section 2 of the 2000 Act as a basis for data sharing.
- 18.2.4 The starting point in relation to implied powers or in relation to section 111 of the 1972 Act must be the power to carry out the fundamental activity to which data sharing is ancillary. If there is no power to carry out that fundamental activity then there can be no basis for implying a power to share data or for relying on section 111 of the 1972 Act.
- 18.2.5 A statutory power must be exercised for the purpose for which it is created. If it is not, the exercise of the power will be ultra vires.

### **18.3 Administrative powers**

- 18.3.1 If a public body does not have the power or vires to collect, use or share data it will be acting unlawfully and the fact that an individual may have consented would not make the activity lawful.
- 18.3.2 Express statutory powers: Express statutory powers can be permissive or mandatory. Express permissive statutory powers (or gateways) to share data include section 115 of the Crime and Disorder Act 1998 (which allows persons to share information with relevant authorities where disclosure is necessary or expedient for the purposes of the Act) and regulation 27 of the Road Vehicles (Registration and Licensing) Regulations 2002 (which, among other things, permits the Secretary of State to make particulars in the vehicle registration register available for use by a local authority for any purpose connected with the investigation of an offence or of a decriminalised parking contravention). Examples of mandatory statutory gateways include: section 17 of the Criminal Appeal Act 1995, which makes it obligatory for a public body to provide information, when requested, to the Criminal Cases Review Commission in connection with the exercise of its functions; and section 6 of the Audit Commission Act 1998, which imposes a legal obligation on the Council to provide relevant information to the Audit Commission.
- 18.3.3 Local authorities are only be able to do what is expressly or by implication authorised by statute. The following general statutory powers are relevant, in addition to the specific powers mentioned above:

- a) Section 111 of the Local Government Act 1972, which provides that a local authority has power to do anything, which is calculated to facilitate, or is conducive or incidental to, the discharge of any statutory functions.
- b) Section 2 of the Local Government Act 2000, which provides that a local authority has power to do anything likely to achieve the promotion or improvement of the economic, social or environmental well-being of the area.

## **18.4 Data Protection Act 1998**

### 18.4.1 The key principles of the Data Protection Act are:-

- a) Personal Data must be processed (e.g. collected, held, disclosed) fairly and lawfully and that processing must satisfy one of the conditions in schedule 2 of the Act. The processing of sensitive data is further protected in that processing must also satisfy at least one of the conditions in schedule 3 of the Act.
- b) Personal Data shall be obtained and processed for only one or more specific and lawful purpose(s).
- c) Personal Data shall be adequate, relevant and not excessive in relation to the specified purpose(s).
- d) Personal Data shall be accurate and kept up to date.
- e) Personal Data shall not be held for longer than is necessary.
- f) Processing of Personal Data must be in accordance with the rights of the individual.
- g) Appropriate technical and organisational measures should protect Personal Data.
- h) Personal data should not be transferred outside the European Union unless adequate protection is provided by the recipient.

18.4.2 With few exceptions the Data Protection Act 1998 requires anyone processing personal information to register with the Information Commissioner.

18.4.3 The registration details include the type of information held, the purpose of use and who the information may be disclosed to. It is therefore essential that anyone considering sharing personal information establishes that their registration covers who they may disclose information to, or what information they may collect (when receiving shared information). If their registration does not cover these matters adequately, amendments must be registered with the Information Commissioner.

18.4.4 The first and second principles of the Data Protection Act are crucial when considering information sharing. In essence, these require that personal information should be obtained and processed fairly and lawfully and that personal information should not be used for a purpose(s) incompatible with the original purpose.

18.4.5 Schedules 2 and 3 of the Act set out conditions that must be met before personal information can be processed fairly and lawfully. For personal information to be processed lawfully, one of the conditions in Schedule 2 must be met. For sensitive personal information, one of the conditions in Schedule 3 must also be met.

18.4.6 Sensitive information, as defined by the Act, includes information concerning a person's physical or mental health; sexual life; ethnicity or racial origin; political

- opinion; trade union membership; criminal record or details of alleged offences etc.
- 18.4.7 In order for there to be no misunderstanding, on anyone's part, it is advisable for the 'collector' of the information to ensure that the person is made fully aware of why the information is needed, what will be done with it, who will have access to it, their rights and if appropriate seek the informed consent of the individual concerned before sharing that information.
- 18.4.8 There are circumstances where information can be shared even if informed consent has not been given. These include the following:
- a) Section 29 of the Act permits disclosure for the purposes of prevention or detection of crime, or apprehension or prosecution of offenders, and where those purposes would be likely to be prejudiced by non-disclosure.
  - b) Disclosure is also permitted where information has to be made public, or where disclosure is required by law.
- 18.4.9 For the purposes of the common law duty of confidentiality, if there is no informed consent, this is the point where the need for confidentiality would have to be balanced against countervailing public interests – again preventing crime is accepted as one of those interests. See further the more detailed discussion of confidentiality, below.
- 18.4.10 For the purposes of the Human Rights Act 1998, Article 8 – Right to respect for private and family life, would need to be considered. See the more detailed discussion of article 8, below.
- 18.4.11 The Data Protection Act gives individuals various rights in respect of their own personal data held by others, namely the right to:-
- a) access their own information (subject access request).
  - b) take action to rectify, block, erase or destroy inaccurate data.
  - c) prevent processing likely to cause unwarranted substantial damage or distress.
  - d) prevent processing for the purposes of direct marketing.
  - e) to be informed about automated decision taking processes.
  - f) take action for compensation if the individual suffers damage.
  - g) apply to the Information Commissioner or the court to have their rights under the Act enforced.
- 18.4.12 Section 7 of the Act, gives an individual the right to access the information held about themselves, irrespective of when the information was recorded or how it is stored (manual or electronic).
- 18.4.13 Disclosure of information held on an individual's record that identifies or has been provided by a third party is subject to certain restrictions.
- 18.4.14 The Act provides the holder of the information a limited number of exemptions to decline/refuse access to an individual's record which are set out under Part IV of the Act.
- 18.4.15 The Data Protection Act 1998 does not apply to personal information relating to a

deceased person.

- 18.4.16 The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 apart from section 3.1.(f) which continues to provide a right of access to the health records of deceased person made by their personal representatives and others having a claim on the deceased's estate.
- 18.4.17 In all other circumstances, disclosure of records relating to the deceased person should satisfy common law duty of confidence.
- 18.4.18 **Schedule 2** of the Data Protection Act 1998 specifies conditions relevant for the processing of any personal data, namely:-
- a) The data subject has given his/her consent to the processing, or
  - b) The processing is necessary for the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract, or
  - c) The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract, or
  - d) The processing is necessary to protect the vital interests of the data subject.
  - e) The processing is necessary-for the administration of justice for the exercise of any functions conferred on any person by or under any enactment for the exercise of any functions of the Crown, a Minister of the Crown or a government department for the exercise of any other functions of a public nature exercised in the public interest by any person, or
  - f) The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.
- 18.4.19 **Schedule 3** of the Data Protection Act 1998 specifies additional conditions relevant for the processing of sensitive personal data, namely:-
- a) The data subject has given his/her consent, or
  - b) Processing of sensitive personal data is necessary:-
  - c) By right or obligation under law, or
  - d) To protect specific vital interests of the individual or other persons, where consent cannot be given by or on behalf of the individual or,
  - e) In the course of legitimate activities of specified non-profit organisations, with extra safeguards, or
  - f) Information already publicly released by the individual.
  - g) Legal, judicial, government or crown reasons, or
  - h) Medical purposes, or
  - i) To monitor equality of opportunity, or
  - j) By order of the Secretary of State.

## **18.5 Human Rights Act 1998 and European Convention on Human Rights**

- 18.5.1 The Human Rights Act 1998(the HRA) gives further effect to the principal rights guaranteed by the European Convention on Human Rights (the Convention). In general, it is unlawful under the HRA for a public authority to act inconsistently with any of the Convention rights.
- 18.5.2 Article 8.1. of the European Convention on Human Rights (given effect via the Human Rights Act 1998), provides that “everyone has the right to respect for his private and family life, his home and his correspondence.”
- 18.5.3 This is however, a qualified right i.e. there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights.
- 18.5.4 Article 8.2 of the European Convention on Human Rights provides “there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”
- 18.5.5 In the event of a claim arising from the Act that an organisation has acted in a way which is incompatible with the Convention rights, a key factor will be whether the organisation can show, in relation to its decision(s) to have taken a particular course of action:-
- a) that it has taken these rights into account;
  - b) that it considered whether any breach might result, directly or indirectly, from the action, or lack of action;
  - c) if there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights;
  - d) (if qualified rights) whether the organisation has proceeded in the way mentioned below. “Evidence of the undertaking of a 'proportionality test', weighing the balance of the individual rights to respect for their privacy, versus other statutory responsibilities e.g. protection of others from harm, will be a significant factor for an organisation needing to account for its actions in response to claims arising from the Act”.

## **18.6 Crime and Disorder Act 1998**

- 18.6.1 The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area.
- 18.6.2 Section 115 of the Act provides a power (not a statutory duty) to exchange information between partners where disclosure is necessary to support the local Community Safety Strategy or other provisions in the Crime and Disorder Act. This power does not over ride other legal obligations such as compliance with the Data Protection Act (1998), the Human Rights Act (1998) or the common law of confidentiality.

- 18.6.3 Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient, for the purposes of the Act.
- 18.6.4 Whilst all agencies have the power to disclose, section 115 does not impose a requirement on them to exchange information, and responsibility for the disclosure remains with the agency that holds the information. It should be noted, however, that this does not exempt the provider from the requirements of the second Data Protection principle.

## **18.7 Common Law Duty of Confidentiality**

- 18.7.1 All staff working in both the public and private sectors should be aware that they are subject to a Common Law Duty of Confidentiality, and must abide by this.
- 18.7.2 'In Confidence'... Information is said to have been provided in confidence when it is reasonable to assume that the provider of that information believed that this would be the case, in particular where a professional relationship may exist e.g. doctor/patient, social worker/client; lawyer/client etc.
- 18.7.3 The duty of confidence only applies to person identifiable information and not to aggregated data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specific individual.
- 18.7.4 The duty of confidentiality requires that unless there is a statutory requirement or other legal reason to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g. to protect others from harm).
- 18.7.5 Whilst it is not entirely clear under law whether or not a common law duty of confidence extends to the deceased, the Department of Health and relevant professional bodies accept that there is an ethical duty to respect the confidentiality of the dead.
- 18.7.6 Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained before disclosure of their information. In addition, the data protection principles (including the requirements of Schedules 2 and 3 of the Data Protection Act 1998) apply whether or not the information was provided in confidence.
- 18.7.7 Where it is judged that an individual is unable to provide informed consent (due to age or condition), then in order to avoid a breach of the common law duty of confidentiality it will usually be necessary to consider whether in order to avoid a breach of the Data Protection Act, Schedule 2 and (in the case of sensitive personal data) Schedule 3 to the Data Protection Act 1998 must be satisfied, notwithstanding the absence of consent.. Processing might for instance be lawful

as being in the vital interest of the individual. 'Public functions' as outlined in schedule 2, and 'medical purposes' as outlined in schedule 3 of the Data Protection Act 1998 are also likely to be very relevant.

## **18.8 Regulation of Investigatory Powers Act 2000**

18.8.1 The Regulation of Investigatory Powers Act 2000 primarily deals with the acquisition and disclosure of information relating to the interception of communications, the carrying out of surveillance and the use of covert human intelligence. It is unlikely that this Act will have any implications on the sharing of personal information.

## **18.9 Caldicott**

18.9.1 Although not a statutory requirement, NHS and Social Care organisations are committed to the Caldicott principles which encapsulate the above mentioned statutes when considering whether confidential information should be shared. These are:-

- a) Justify the purpose(s) for using personal information.
- b) Only use personal information when absolutely necessary.
- c) Use the minimum amount of personal information that is required.
- d) Access to personal information should be on a strict need to know basis.
- e) Everyone with access to personal information must be aware of his/her responsibilities.
- f) Everyone with access to personal information must understand and comply with legislation that governs personal information.

## **18.10 The Children Act 2004**

18.10.1 The Children Act 2004 created the legislative framework for developing more effective and accessible services focused around the needs of children, young people and families by ensuring co-operation, clearer accountability and safeguarding of children. The key event which led to these proposals for fundamental change was the death of Victoria Climbié. This demonstrated that there were major flaws within the systems and structures for safeguarding and ensuring the welfare of children and young people.

18.10.2 Main provisions of the Act:

- a) A Children's Commissioner
- b) A new duty on agencies to co-operate to improve the well-being of children and young people
- c) A duty to safeguard and promote the welfare of children
- d) A power to set up a new database with information about children
- e) Local Safeguarding Children Boards
- f) Children and young people's plans

- g) Director of Children's Services and Lead Member
- h) A framework for inspection and joint area reviews
- i) New powers of intervention in failing authorities
- j) A duty to promote the educational achievement of looked after children
- k) Ascertaining children's wishes
- l) Additional items include: private fostering, child minding and day care, adoption review panels, grants in respect of children and families and Child Safety Orders.

## **18.11 Summary of the Children Act 2004**

18.11.1 The following is a brief account of the key parts of the Act that specifically relate to the Change for Children programme in England.

### **Children's Commissioner – Part 1**

- 18.11.2 Sections 1-9 provide for the establishment of a new Children's Commissioner for England, who will also have a role across the UK for reporting on non-devolved matters, working closely with counterparts in Wales, Scotland and Northern Ireland. The Commissioner's job will be to raise awareness of the best interests of children and young people and to report annually to Parliament, through the Secretary of State, on his findings.
- 18.11.3 Section 2 makes clear that the Commissioner will not act as a last court of appeal for individual cases. Instead the Commissioner will look at how bodies, including Government and the public and private sectors, listen to children and young people. The Commissioner will be able to highlight failures in complaints procedures and make recommendations for improvements.
- 18.11.4 Section 3 gives the Commissioner freedom to look at an individual case with wider implications, for the purpose of learning broader lessons to inform public policy. Subject to the appointment process we expect the first Commissioner to be in place by April 2005.

### **Children's Services in England – Part 2**

- 18.11.5 Section 10 establishes a duty on Local Authorities to make arrangements to promote co-operation between agencies in order to improve children's well-being, defined by reference to the five outcomes and a duty on key partners to take part in those arrangements. It also provides a new power to allow pooling of resources in support of these arrangements.
- 18.11.6 Section 11 creates a duty for the key agencies who work with children to put in place arrangements to make sure that they take account of the need to safeguard and promote the welfare of children when doing their jobs.
- 18.11.7 Section 12 allows further secondary legislation and statutory guidance to be made with respect to setting up indexes that contain basic information about children and young people to help professionals in working together to provide early support to

children, young people and their families. Case details are specifically ruled out.

- 18.11.8 Sections 13-16 require that Local Authorities set up statutory Local Safeguarding Children Boards and that the key partners take part.
- 18.11.9 Section 17 and the associated repeals in Schedule 5 establish a single Children and Young People's Plan (CYPP) to replace a range of current statutory planning. Details of what the CYPP should cover will be set out in further secondary legislation and supported by guidance. There will be no requirement for the Secretary of State to approve the plan and Local Authorities categorised as excellent under Comprehensive Performance Assessment will be exempt from the requirement.
- 18.11.10 Sections 18 & 19 require Local Authorities to put in place a Director of Children's Services and Lead Member to be responsible for, as a minimum, education and children's social service functions. Local Authorities have discretion to add other relevant functions, for instance leisure or housing, to the role if they feel it is appropriate.
- 18.11.11 Sections 20-24 require an integrated inspection framework to be established by the relevant inspectorates to inform future inspections of all services for children. They also make provision for regular Joint Area Reviews to be carried out to look at how children's services as a whole operate across each Local Authority area.

#### **Other provisions – Part 5**

- 18.11.12 Sections 44-47 put stronger requirements on Local Authorities to manage and monitor the current statutory notification scheme for private fostering arrangements. They also allow for a registration scheme to be set up if the notification arrangements prove to be inadequate.
- 18.11.13 Section 49 allows for the secondary legislation to be made to bring in a minimum fostering allowance.
- 18.11.14 Section 50 makes changes to allow consistent intervention across Local Authority education and children's social service functions where it is shown to be necessary.
- 18.11.15 Section 52 puts a duty on the Local Authority in its role as the corporate parent to promote the educational achievement of looked after children. This will ensure that decisions on issues such as placement and stability support better educational achievement.

## **19 APPENDIX B - Checklist of legal considerations**

### **19.1 Purpose**

19.1.1 This is meant as a guide to assist in determining how to establish the legal basis for data sharing. A new data sharing initiative may involve two or more public bodies who wish to share information with each other in order to set up a central database of useful information that they may each access. This information could be, for example, limited to up-to-date client names and addresses. Alternatively, it could be information about children thought to be at risk of serious physical harm. Consideration will need to be given to the following legal issues:

### **19.2 Vires issues**

19.2.1 Does the body that it is to hold and administer the database (the data controller) have the vires/power to do so? In determining this question careful consideration will need to be given to the existing legal powers that that body has and whether these powers extend to the holding and operation of the new database.

19.2.2 Is the existing data that is to be shared subject to relevant statutory prohibitions whether express or implied? For example, the DCA takes the view that the sharing of information relating to council tax may be subject to a relevant statutory prohibition that would make any sharing of that information ultra vires (the Council reserves its position on this issue, pending further legal advice).

19.2.3 Even if there are no relevant statutory restrictions, do the bodies sharing the data have the vires to do so? This will involve careful consideration of the extent of express statutory, implied statutory and common law powers.

19.2.4 If there is no existing legal power for the proposed data collection and sharing, then consideration should be given to requesting the Government to enact new legislation.

### **19.3 Human Rights Act issues**

19.3.1 Is Article 8 of the ECHR engaged i.e. will the proposed data collection and sharing interfere with the right to respect for private and family life, home and correspondence? If the data collection and sharing is to take place with the consent of the data subjects involved, Article 8 will not be engaged.

19.3.2 If Article 8 of the ECHR is engaged, is the interference (a) in accordance with the law; (b) in pursuit of a legitimate aim; and (c) necessary in a democratic society?

### **19.4 Common law of confidence issues**

19.4.1 Is the information confidential i.e. does it (a) have the necessary quality of confidence; (b) was the information in question communicated in circumstances giving rise to an obligation of confidence?; (c) has there been an unauthorised use of that material? Consider also whether the information has been obtained subject to statutory obligations of confidence. If the data collection and sharing is to take place with the consent of the data subjects involved, then the data sharing will not involve a breach of the duty of confidence.

19.4.2 If the information is confidential is there an overriding public interest that justifies its disclosure? The law on this aspect overlaps with that relating to Article 8 of the

ECHR.

**19.5 Data Protection Act issues**

- 19.5.1 Do the eight principles in Schedule 1 of the DPA apply i.e. is the information personal data held on computer or as part of a relevant filing system or an accessible record?
- 19.5.2 If Schedule 1 of the DPA applies, can the requirement of fairness in the First Data Protection Principle be satisfied?
- 19.5.3 Can one of the conditions in Schedule 2 be satisfied? Of particular relevance to public sector data sharing are the requirements in paragraph 5 that relate to public functions; and the requirement in paragraph 6, that involves a balance between the interests of the data subject and the interests of the body that shares and/or that receives the data.
- 19.5.4 If the data are sensitive personal data can one of the conditions in Schedule 3 also be satisfied? Paragraph 7 which is in similar terms to paragraph 5 of Schedule 2 may be applicable.
- 19.5.5 Can the requirement of compatibility that is in the Second Data Protection Principle be complied with?
- 19.5.6 Do any of the exemptions that are set out in the DPA apply?

## **20 APPENDIX C - Consent: Guidance notes**

### **20.1 Consent**

- 20.1.1 In the past consent has all too often either been assumed or implied. Unfortunately, when something goes wrong it has been very difficult to prove if consent was actually given. Today it is almost always recommended that consent should be explicit e.g. in writing.
- 20.1.2 In order to facilitate the sharing of personal information (without statutory grounds) it is essential that careful consideration should be given to obtaining explicit consent whenever possible, regardless of the person's age.
- 20.1.3 The key criterion that must be satisfied when obtaining consent is: 'that the person concerned should be mentally and emotionally capable of giving informed consent of his/her own free will'.
- 20.1.4 For the consent to be valid, the person concerned must:-a) Have the capacity to take a particular decision, and b) Have received sufficient information to make a decision, and c) Not be acting under duress.
- 20.1.5 Consent may be given non-verbally, orally or in writing. In order to avoid any confusion or misunderstanding at a later date, non-verbal or oral consent should be witnessed and the details of the witness recorded.
- 20.1.6 To give valid informed consent, the person needs to understand in broad terms why their information needs to be shared, what type of information may be involved and who that information may be shared with.
- 20.1.7 The person should also be advised of their rights with regard to their information, namely:-
- a) The right to withhold their consent.
  - b) The right to place restrictions on the use of their information.
  - c) The right to withdraw their consent at any time.
  - d) The right to have access to their records.
- 20.1.8 As well as discussing consent with the person, it is seen as good practice that the person should also be given such information in written form, in an appropriate format e.g. language, Braille.
- 20.1.9 To be valid, consent must be given voluntarily and freely, without any pressure or undue influence being exerted on the person by those seeking consent or family and friends of the person whose consent is being sought.
- 20.1.10 In general once a person has given consent, that consent may remain valid for an indefinite duration unless the person subsequently withdraws that consent.
- 20.1.11 For the purpose of the General Protocol, the consent duration should be time limited to the specific 'piece of work' that is being proposed.
- 20.1.12 It should be considered good practice to seek 'fresh' consent once the original piece of work is completed or there are significant changes in the circumstances of the person or work being undertaken.

- 20.1.13 If a person makes a voluntary and informed decision to refuse consent for their personal information to be shared, this decision must be respected unless there are sound legal grounds for not doing so.
- 20.1.14 A person, having given their consent, is entitled at any time to subsequently withdraw that consent. Like refusal, their wishes must be respected unless there are sound legal grounds for not doing so.
- 20.1.15 If a person refuses or withdraws consent, the consequences should be explained to them, but care must be exercised not to place the person under any undue pressure.

## **20.2 Capacity**

- 20.2.1 For a person to have capacity, he/she must be able to comprehend and retain the information material to the decision and must be able to weigh this information in the decision making process.
- 20.2.2 The BMA has published guidance on the assessment of capacity.

## **20.3 Young Persons**

- 20.3.1 Section 8 of the Family Law Reform Act entitles young people aged 16 or 17, having capacity, to give informed consent.
- 20.3.2 Following the case of Gillick v West Norfolk and Wisbech AHA [1986] AC 122, the courts have held that young people (below the age of 16) who have sufficient understanding and intelligence to enable them to understand fully what is involved will also have capacity to consent.
- 20.3.3 It should be seen as good practice to involve the parent(s) of the young person in the consent process, unless this is against the wishes of the young person.

## **20.4 Parental Responsibility**

- 20.4.1 The Children Act 1989 sets out persons who may have parental responsibility, these include:-
  - a) The child's parents if married to each other at the time of conception or birth;
  - b) The child's mother, but not the father if they were not so married unless the father has acquired parental responsibility via a court order or a parental responsibility agreement or the couple subsequently marry;
  - c) The child's legally appointed guardian;
  - d) A person in whose favour the court has made a residence order in respect of the child;
  - e) A local authority designated in a care order in respect of the child;
  - f) A local authority or other authorised person who holds an emergency protection order in respect of the child.

(Note: Foster parents or guardians do not automatically have parental responsibility)

- 20.4.2 Whilst, under current law, no-one can provide consent on behalf of an adult in order to satisfy the Common law requirement, it is generally accepted by the courts

that decisions about treatment, the provision of care, and the disclosure of information, should be made by those responsible for providing care and that they should be in the best interests of the individual concerned.

## **20.5 Obtaining Consent**

20.5.1 For consent to be valid a number of criterion must be satisfied (see Consent 1. above). In order for consent to be obtained lawfully it is essential that all persons who may be expected to obtain consent for the sharing of personal information receive appropriate training and that under normal circumstances only those employees who have received training and been approved by management should seek consent.

## **20.6 Disclosure of Personal Information**

20.6.1 The passing of personal information without either statutory cause or the consent of the person concerned, places both the agency and the individual member of staff at risk of prosecution.

20.6.2 It is therefore essential that all agencies who are party to the General protocol have in place policies and procedures governing who may disclose personal information and that such policies/procedures are communicated to all of their employees.

## **20.7 Disclosure with consent**

20.7.1 Only staff who have been authorised to do so should disclose personal information about an individual service user.

20.7.2 Prior to disclosing personal information about an individual, the authorised member of staff should check the individual's file/record in order to ascertain:-

- a) that consent to disclose has been given, and
- b) the consent is applicable for the current situation, and
- c) any restrictions that have been applied.

20.7.3 On the first instance of disclosure with respect to the particular situation, the person making the disclose should forward a copy of the individual's consent form to the receiving agency.

20.7.4 Disclosure of personal information will be strictly on a need to know basis and in accordance with any agreed Individual Protocol.

20.7.5 All information disclosed should be accurate and factual. Where opinion is given, this should be made clear to the recipient.

20.7.6 On disclosing personal information to another agency, a record of that disclosure should be made on the individual's file/record, this should include:-

- a) When the disclosure was made.
- b) Who made the disclosure.
- c) Who the disclosure was made to.
- d) How the disclosure was made.

- e) What was disclosed.

20.7.7 The recipient of information should record:-

- a) The details of the information received.
- b) Who provided it.
- c) Any restrictions placed on the information that has been given e.g. 'not to be disclosed to the service user'.

## **20.8 Disclosure without consent**

20.8.1 It is recognised that in certain emergency situations, such as vulnerable person investigations, speed is of the essence and inter-agency communication is of paramount importance and obtaining consent to disclose may be neither practical or expedient.

20.8.2 Staff involved in such situations all too often become completely focused on the core issue and often lose sight of the need to exercise caution when disclosing personal information.

20.8.3 Frequently staff are under the impression that the statute which enables them to undertake a particular duty also gives them the automatic right to collect, process and disclose whatever information they need. With very few exceptions, this is not the case.

20.8.4 The Data Protection Act 1998 is the key legislation governing the collection, processing and disclosure of personal information and almost all other statutes refer to it.

20.8.5 Disclosure of personal information without consent must be justifiable on statutory grounds, or a meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.

20.8.6 All agencies who are party to the General Protocol should set in place policies and procedures that deal specifically with the sharing of information under emergency situations e.g. major disaster.

20.8.7 All agencies should designate a person who has the knowledge and authority to take responsibility for making decisions on disclosure without consent. This person should hold sufficient seniority within the agency with influence on policies and procedures. Within the health and social care agencies it is expected that this person will be the Caldicott Guardian.

20.8.8 If disclosure is made without consent, the person making the disclosure must:-

- a) Advise the recipient accordingly.
- b) Record the full details of the disclosure that has been made, including the reason why the decision to disclose was taken (statute or exemption); who made the disclosure and to who it was disclosed to.

20.8.9 The recipient of information that has disclosed without consent should record:-

- a) The details of the information received.
- b) Who provided it.
- c) Any restrictions placed on the information that has been given e.g. 'not to be disclosed to the service user'.
- d) That the information was provided without consent, and the reason(s) why (if known).

## **20.9 Recording Consent**

20.9.1 All agencies should have in place a means by which an individual, or their guardian/representative, can record their explicit consent to personal information being disclosed and any limitations, if any, they wish to place on that disclosure.

20.9.2 The consent form should indicate the following:-

- a) Details of the agency and person obtaining consent.
- b) Details to identify the person whose personal details may/will be shared.
- c) The purpose for the sharing of the personal information.
- d) The organisation(s)/agency(ies) with whom the personal information may/will be shared.
- e) The type of personal information that will be shared.
- f) Details of any sensitive information that will be shared.
- g) Any time limit on the use of the consent.
- h) Any limits on disclosure of personal information, as specified by the individual.
- i) Details of the supporting information given to the individual.
- j) Details of the person (guardian/representative) giving consent if appropriate.

20.9.3 The individual or their guardian/representative, having signed the consent, should be given a copy for their retention.

20.9.4 The consent form should be securely retained on the individual's file/record and that relevant information is recorded on any electronic systems used in order to ensure that other members of staff are made aware of the consent and any limitations.

## **20.10 Use Of Personal Information For Purposes Other Than Agreed**

20.10.1 It is recognised that agencies who are party to the General Protocol may fulfil a number of roles. In fulfilling one particular role, they may be given privileged access to personal information which they may subsequently find could assist them in another role or be of wider interest to their organisation.

20.10.2 Personal information shared under this General Protocol will have been disclosed for a specific purpose, as defined in the Individual Protocol, and as such must only be used for that purpose.

20.10.3 Agencies wishing to use personal information given to them under the General Protocol for any purpose other than that defined in the Individual Protocol, or who may wish to disclose that information to any person other than those authorised to receive that information, must:-

- a) Inform the originator of their intention to use the information provided for a different purpose.
- b) Obtain explicit consent from the individual(s) concerned before processing such information.

20.10.4 If the originator of the personal information considers that the purpose for which the information is proposed to be used is likely to be detrimental to their agency, or the individual(s) whose personal information it is proposed to use object, then that information should not be used for the proposed purpose.

20.10.5 Agencies wishing to use personal information that has been provided to them under the General Protocol for research or statistical purposes should ensure that policies and procedures are in place to guarantee that such personal information is anonymised.

## **21 APPENDIX D - Protocol Management Procedures**

### **21.1 Formal approval and adoption of the protocol**

- 21.1.1 The General Information Sharing Protocol is a product of the London Borough of Islington and has been endorsed by the Islington Strategic Partnership.
- 21.1.2 A General Information Sharing Protocol will be established between Islington Council and any agency commissioned to provide a service on behalf of Islington Council, where there is a need to share personal information about service users, e.g. home care providers, residential care providers. The protocol will be supplementary to any contract or service level agreement between Islington Council and the agency concerned.
- 21.1.3 Individual Information Sharing Agreements will be drawn up as necessary. These will relate to specific groups of service users and/or specific projects that involve the sharing of personal information. These agreements will be compliant with the General Information Sharing Protocol.

### **21.2 Circulation of the Protocol**

- 21.2.1 The protocol will be introduced to managers, front line and field workers following internal agency training plans and procedures.
- 21.2.2 Copies of the protocols will be circulated to all relevant staff, in line with each organisation's internal distribution procedures and guidelines. Wherever possible, the document will be available to staff online.
- 21.2.3 A strategy for disseminating the protocol 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 information.
- 21.2.4 The protocols will be published, wherever possible, on the web sites of the organisations party to the protocol and made available at public information points. Each partner organisation will keep sufficient copies to enable the document to be readily available to members of the public who require it.

### **21.3 Monitoring and Reviewing procedures**

- 21.3.1 The protocol will be subject to regular formal review.
- 21.3.2 Legal advice will always be sought before any major changes to the protocols are made.
- 21.3.3 Each protocol will set out the particular arrangements for the review of that protocol. These will include details of:
- The body responsible for reviewing and agreeing changes
  - The date of the initial review and the review frequency
  - The body or individual(s) who will co-ordinate the review.
- 21.3.4 Following the introduction of a protocol, its use and application will be closely

monitored until the date of the first formal review. The date of introduction of a protocol until the date of its first formal review will be known as the pilot phase. The length of this period and the individual(s) responsible for monitoring its use during the pilot phase will be specified in all protocols. During this period, changes will only be considered if the issues and problems identified are felt to be a significant barrier to information exchange.

#### **21.4 The use and effectiveness of the protocol will be evaluated in a number of ways.**

21.4.1 Staff in all organisations will be required to log and report responses and behaviour that they believe are not in accordance with the protocol. During the pilot phase, breaches will be analysed frequently to ensure that problems with the implementation of the protocol are addressed before they become a major issue.

21.4.2 Telephone surveys will be carried out within each organisation to establish how familiar members of staff are with the protocol. Staff will be asked to report on their awareness of and access to the protocol and internal procedures arising from it; training they have received in relation to the protocol and any further training needs arising; the methods and extent to which they have applied the protocol; and any problems they have encountered.

21.4.3 Complaints received by organisations will be analysed to determine whether they relate to a breakdown or inadequacy of the protocol. All organisations party to the protocol will establish a procedure by which complaints regarding inappropriate use or disclosure of information are reported to the body responsible for the security of that information.

21.4.4 Prior to each formal review of the protocol, a survey will target all stakeholder groups. The survey will seek to establish:

- The ease of application of the procedures
- The effectiveness of the protocol in encouraging organisations to share information
- Difficulties encountered in applying the protocol
- Proposals for improving procedures
- The contribution of the protocol to achieving the objectives of relevant strategies.

21.4.5 A survey will also be designed to test public awareness of protocol and associated material. Advice will be taken from the public information officers and various voluntary sector organisations established to represent or work with service users.

#### **21.5 Reporting Breaches of the Protocol**

21.5.1 During the pilot phase, all breaches are to be logged, investigated, and the outcome noted. The continued need to do so after the pilot phase will be examined as part of the review process.

21.5.2 The following types of incidents will be logged:

- Refusal to disclose information
- Conditions being placed on disclosure
- Delays in responding to requests
- Disclosure of information to members of staff who do not have a legitimate reason for

- access
- Non-delivery of agreed reports
- Inappropriate or inadequate use of procedures e.g. insufficient information provided
- Disregard for procedures
- The use of data/information for purposes other than those agreed in the protocol
- Inadequate security arrangements.

## **21.6 Breaches noted by members of staff:**

- 21.6.1 A member of staff working on behalf of any organisation party to the protocol who becomes aware that the procedures and agreements set out in the protocol are not being adhered to, whether within their own or a partner organisation, should first raise the issue with the line manager responsible for the day-to-day management of the protocol.
- 21.6.2 The manager should record the issue and check whether the concern is justified. If the manager concludes that the protocol is being breached, he or she should first try to resolve it informally. If the matter can be resolved in this way, the outcome should be noted and forwarded to the designated person (the person responsible for monitoring the protocol during the pilot phase) who should file the details in a 'breaches log'.
- 21.6.3 The line manager should inform the member of staff who raised the issue of the outcome prior to submitting the issue to the designated person. If the member of staff is not satisfied with the response they should be able to record their comments on the form prior to submission.
- 21.6.4 A time limit of 10 days should be allowed for informal negotiation. At the end of this period, the details of any actions and the outcome of negotiations should be noted and passed to the designated person for logging and for reporting.

## **21.7 Breaches alleged by a member of the public:**

- 21.7.1 Any complaint received by, or on behalf of, a member of the public concerning allegations of inappropriate disclosure of information will be dealt with in the normal way by the internal complaints procedures of the organisation who received the complaint: Any disciplinary action will be an internal matter for the organisation concerned.
- 21.7.2 In order to monitor adherence to and use of the protocol, procedures should be established within each organisation by which complaints relating to the inappropriate disclosure of information is passed by the complaints officer to the officer designated to deal with breaches of the protocol. The designated officer should report any complaints of this nature to the equivalent officer in each agency.
- 21.7.3 All alleged breaches of the protocol, whether proven or not, should be analysed as part of the formal review of the protocol.

## TEMPLATES

### **22 Individual Information Sharing Agreement: Template**

## INDIVIDUAL INFORMATION SHARING AGREEMENT

---

### The Agreement

## Document History

This document has been distributed to:

Version	Date	Author	Released to	Comments

This document requires the following approvals

Date	Version	Name	Role

## **CONTENTS**

1. Purpose of the agreement
2. Specific purpose for sharing information
3. Legal basis for sharing
4. Description of arrangements including security matters.
5. Agreement

## **PURPOSE OF THE AGREEMENT**

This Individual Protocol is made under the General Information Sharing Protocol and serves the purpose for specific information sharing.

This agreement has been developed to:

- a) Define the specific purposes for which the signatory agencies have agreed to share information.
- m) Describe the roles and structures that will support the exchange of information between agencies.
- n) Set out the legal gateway through which the information is shared, including reference to the Human Rights Act 1998 and the common law duty of confidentiality.
- o) Describe the security procedures necessary to ensure that compliance with responsibilities under the Data Protection Act and agency specific security requirements.
- p) Describe how this arrangement will be monitored and reviewed.
- q) (N.B Add any additional purposes which may be specific to the particular requirement)

**The signatories to this agreement will represent the following agencies/bodies:**

Start typing here.

*List here all the agencies involved in delivering this particular agreement*

## **SPECIFIC PURPOSE FOR SHARING INFORMATION**

r) Start typing here.

*Use the sections 1, 2 and 3 of the Proposal document as the basis for this. Cut and paste where appropriate.*

### **Management Summary**

a) Start typing here.

*[This greyed out text should be deleted and replaced]*

*Describe the purpose and scope of the information sharing arrangement:*

*This should provide a high level summary of the proposed arrangement:*

- Provide a brief description of the purpose of the arrangement. This should be full enough to give someone unfamiliar with the requirement a clear understanding of what it is about in general terms.*
- Indicate the agencies that will be signatories to the arrangement*
- Provide summary details of information that will be disclosed (e.g. “physical descriptions of wanted persons”, “addresses of victims of distraction burglaries”)*
- Provide summary details of any information that will be received from other signatories.*

*Remember that this section will be used by a wide readership to gain a basic understanding of what the proposal is all about. The content here can also be used as the preamble to the eventual agreement.*

## Objectives

### What are the objectives of the partnership?

a) Benefits [Start typing here].

How does the arrangement meet any corporate objectives?

How does it help achieve any obligations or duties that your partnership has?

Etc

### Partner Agency(ies) Benefits

a) Start typing here.

### Citizen Benefits

a) Start typing here.

(This relates to members of the public. The benefits listed must be directly attributable to the information sharing and must be sufficiently detailed to make sense to someone unfamiliar with the requirement (but who has read the summary above). Please note that the benefits to the citizen will be particularly key to determining whether the arrangement can satisfy the legal requirements for information sharing in the public sector.

The content here will feed into both the Legal Basis documentation and the purpose specific agreement.

### How will this information sharing arrangement further those objectives?

a) Start typing here.

*Explain how the arrangement will support the objectives above. Show that the objectives will not be achieved unless information is shared; i.e. there is no other effective means of undertaking the activity.*

## Information to be Shared

### The following information will be shared

a) Start typing here.

*List the items of information to be disclosed and what systems they are derived from. Be as detailed as possible. If the arrangement involves extracting information from systems en masse, it should be possible to specify the criteria by which the records are selected and which fields from which systems will be used. If on the other hand you propose an agreement to make a series of individual disclosures in response to specific requests – sharing offender details at case conferences for instance - it may be necessary to be more general.*

*For each item of data show that it is necessary to share the information in order to support the stated objectives..*

*If there is personal data involved, this information will be used to satisfy the Third Principle of the Data Protection Act in the Legal Basis, (Personal data shall be adequate, relevant.....). It will form the basis for the assessment of protective marking in the Baseline Security Assessment and will also be used in the protocol.*

### Does this include personal data under the Data Protection Act 1998?

a) Yes/No

*Unless the information to be passed is entirely anonymised or statistical, the answer to this will probably be “yes”. However, even if it is anonymised or statistical, you should give careful consideration to the possibility that an individual could nevertheless be identified from it – e.g. if it provides statistics on the ethnicity of crime victims in a limited geographical area it might inadvertently identify someone from an uncommon ethnic group in that locale.*

## **LEGAL BASIS FOR SHARING**

a) Start typing here.

*N.B. This section will justify the supply of data to partners. If the requirement includes the supply of partner data in both directions, the both partners need to establish their own legal power to share with the service.*

### **First Principle**

The first Data Protection principle states that data must be processed lawfully and fairly.

#### **Lawfully**

a) Start typing here.

*A public authority must have some legal power entitling it to share the information and the purpose of this section is to indicate the primary legal power that is being invoked to share this information.*

#### *Statutory Duties*

*If the partner wishes to disclose personal information for purposes relating to their duties, then the statutory powers to do so need to be indicated.*

#### *Common Law*

*In general terms, if the sharing of the information is for purposes of undertaking public duties and the remaining sections of the DPA are satisfied, then it may be lawful. The purpose for sharing will already have been made out by you in the first stage of this process, the "Proposal". Therefore you will already be clear if the reason for sharing is sufficiently related to a policing purpose.*

#### **Duty of Confidence**

a) Start typing here.

*If the service has received any information in confidence, you almost certainly have a Duty of Confidence towards the data subject. You will need to indicate how any duty of confidence might be overridden or does not apply.*

*When making decisions in this area, consider the original circumstances in which the information that is going to be shared, together with the type of information it is. You will also need to consider the public interest test.*

#### **Fair Processing**

a) Start typing here.

*When data is obtained from data subjects, you need to ensure, so far as practicable, that the data subjects have, are provided with, or have made readily available to them, the following information: -*

*(a) The identity of the data controller (the person handling the data)*

*(b) If the data controller has nominated a representative for the purposes of the Act, the identity of that representative*

*(c) The purpose or purposes for which the data are intended to be processed.*

*(d) Any further information which is necessary, taking into account the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.*

### **Legitimate Expectation**

a) Start typing here.

*An individual's expectation as to how information given to a public body will be used will be relevant in determining whether the first data protection principle has been complied with. In this section you will need to indicate how the information sharing arrangement is consistent with the legitimate expectations of the data subject. Only in rare circumstances will there be difficulty in showing legitimate expectation.*

### **Human Rights - Article 8: The Right To Respect For Private And Family Life, Home And Correspondence**

a) Start typing here.

*There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. You will need to indicate how the Article 8 of the Human Rights Act is to be satisfied*

*Article 8(1) rights are not absolute and should be weighed against the public interest, which may justify an interference with those rights. In conducting what is a balancing exercise between the rights of the individual and the interests and the good of the public at large, you must identify, how the information sharing is:*

- In pursuit of a legitimate aim (e.g. preventing or reducing crime – under a power of statute or common law)*
- Proportionate*
- Appropriate and necessary to a democratic society*

*Your argument may turn on the beneficial effects of the information sharing to the majority of citizens. It may be useful to rehearse the citizen benefits laid out in your Proposal*

document. It may be useful to use the bullet points above as the headings and address each one in turn.

### **Schedule 2, Data Protection Act 1998**

a) Start typing here.

*In addition to the legal criteria set out above, the individual information sharing arrangement must satisfy **at least one** condition in Schedule 2 of the Data Protection Act in relation to personal data. Indicate the Schedule 2 conditions that are satisfied:*

- a) The data subject has consented to the processing*
- b) The data processing is necessary for Compliance with any legal obligation to which the data controller is subject other than one imposed by contract*
- c) The exercise of functions conferred under statute*
- d) The purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms of legitimate interests of the data subject*

*It may not always be practical or even possible to obtain consent before sharing information and it is not a prerequisite, as long as another condition is satisfied. Moreover consent should never be sought unless you are in a position to respect the refusal to grant consent.*

### **Schedule 3, Data Protection Act 1998**

a) Start typing here.

*If the information is “sensitive” (that is, where it relates to the race, ethnic origin, political opinions, religion or belief system, membership of a trades union, physical/mental health or sexual life, the commission or alleged commission of any offence, proceedings relating to the offence) you must satisfy at least one condition in Schedule 3. You need to indicate how the Schedule 3 Condition is satisfied.*

*(If the information intended for sharing is not “sensitive” simply state – “No sensitive information is subject to sharing for the purposes of this agreement”).*

## **Second Principle**

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

a) Start typing here.

*You need to indicate how the agreement complies with the second data principle. This should be interpreted as “not contradictory” with the purpose for which it was originally obtained.*

*A statement along the following lines may be sufficient. “The purpose of this agreement is to share personal data for research where there will be no measure or decisions targeted at particular individuals, and the research will not cause substantial damage or distress to Data Subjects. The research supports a the specific public duty of this partner. Therefore, in this case this sharing of information is exempt from the second principle.”*

## **1. Third Principle**

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

a) Start typing here.

*You need to indicate how the agreement complies with the third data principle. Define here precisely what information is to be shared. In completing this section adequately, it should be possible to establish proportionality. If the information to be shared is structured data from an information system, then describe the criteria for selecting the data and list the fields required, giving a brief reason for including each one.*

## **2. Fourth Principle**

Personal data shall be accurate and, where necessary, kept up to date.

a) Start typing here.

*You need to indicate how the agreement complies with the fourth data principle. A statement to the effect that it has been subject to the normal corporate procedures and validation to ensure data quality should be inserted here. E.g. “This information comes from PARTNER corporate systems and is subject to our normal procedures and validations intended to ensure data quality. Any inaccuracies should be notified to the PARTNERNAME.”*

*Where the information is static – e.g. provided as a one-off – it will be the responsibility of the new data controller(the partner) to maintain it in future. If so, insert a statement to that effect. Where the data will be maintained by regular updates, state briefly how these will take place, e.g. frequency of updates and whether individual records will be updated or whether the whole dataset will be replaced.*

## **3. Fifth Principle**

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

a) Start typing here.

*You need to indicate how the agreement complies with the fifth data principle. Indicate, as precisely as possible, how long the information will be kept. As in the Third Principle above, adequate completion of this section helps to establish proportionality of the arrangement. The period specified need not be a fixed period, but could be related to a set of criteria or a review procedure.*

*As for the Second Principle, if the purpose of the sharing or disclosure is research, an exemption to the Fifth Principle could be claimed. In addition, S.33 DPA states, "Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle, be kept indefinitely".*

#### **4. Sixth Principle**

Personal data shall be processed in accordance with the rights of data subjects under this Act.

a) Start typing here.

*You need to indicate how the agreement complies with the sixth data principle.*

- *Partners to this arrangement will respond to any notices from the Information Commissioner that impose requirements to cease or change the way in which data is processed.*
- *Partners will comply with subject access requests in compliance with the relevant legislation.*
- *PARTNER A reserves the right to withdraw right of use of the data at any time.*

#### **5. Seventh Principle**

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

*You need to indicate how the agreement complies with the seventh data principle. (Delete this sentence and leave the following statement regarding Baseline Security). Measures to satisfy the Seventh Principle are detailed in the Baseline Security Assessment document.*

#### **6. Eighth Principle**

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data

a) Start typing here.

*You need to indicate how the agreement complies with the eighth data principle. Confirm that the information is not intended for transfer outside the European Economic Area. If so state this here.*

*If the arrangement does require transfer outside the European Economic Area you should contact your legal team for further instruction / advice.*

## **DESCRIPTION OF ARRANGEMENTS INCLUDING SECURITY MATTERS.**

a) Start typing here.

*This section details the processes to be followed to ensure that this agreement is effective and from which work instructions can be prepared for staff.*

*As a minimum this section should cover the following:*

- For regular flows of information, the process for requesting the information;*
- The source of the information and, where appropriate, how the information will be extracted e.g. Name and address fields from SYSTEM A exported on to floppy disk by PARTNER A personnel;*
- The intended recipients of the information;*
- How confidentiality requirements have been met;*
- What measures will be taken to ensure a record is kept of the information shared;*
- How security incidents will be notified to partners;*
- Arrangements for training and awareness;*
- Confidentiality and Vetting arrangements;*
- How the information will be stored by the partner and the physical security arrangements;*
- Whether the information will be processed on a partner's system and if so, the security arrangements in place;*
- How the information will be transferred to the partner;*
- When and how the information will be disposed;*
- If the agreement incorporates a receipt of information from a partner, detail what the information is in general terms and what the police will do with the information*
- When and how these arrangements will be reviewed.*

## AGREEMENT

The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

As such they undertake to:

- Implement and adhere to the procedures and structures set out in this agreement.
- Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement.
- Engage in a review of this agreement with partners at least annually.

**We the undersigned agree that each agency/organisation that we represent will adopt and adhere to this information sharing agreement:**

<b>Agency</b>	<b>Post Held</b>	<b>Name</b>	<b>Signature</b>	<b>Date</b>