

**EAST LONDON HEALTH & SOCIAL CARE**  
**INTER ORGANISATION GENERAL PROTOCOL**  
**FOR**  
**SHARING INFORMATION**

Document History

Version	Date	Change
1-0	19 <sup>th</sup> April 2003	Draft Version
2-0	14 <sup>th</sup> May 2003	Second Draft Version
3-0	30 <sup>th</sup> July	Third draft - Amended by SP following review and discussion at Caldicott Guardian's Forum, June 2003
4-0	7 October	Fourth draft with legal input
5-0	24 November 2003	Fifth draft after meeting 12 November 2003
6-0		Working draft exchanged between RLB/SP and certain group members on request
7-0	18 December 2003	Final Draft released to Parties in preparation for sign up
8-0	January 2004	As above – for discussion at 27/1/04 Caldicott Forum Meeting
9.0	February 2004	As above –following discussion at 27/1/04 Caldicott Forum Meeting and incorporating three changes suggested by Anne Pietsch (Corp of London)
10.0	August 2005	Review with legal input

## CONTENTS

<b>PARTIES</b>	<b>3</b>
<b>DEFINITIONS</b>	<b>3</b>
<b>1. SECTION 1 – BACKGROUND AND CONTEXT</b>	<b>5</b>
1.1 POLICY CONTEXT	5
1.2 LOCAL CONTEXT	5
1.3 SCOPE	6
1.4 LEGISLATION AND GUIDANCE	6
<b>2. SECTION 2 – INFORMATION SHARING GOVERNANCE</b>	<b>7</b>
2.1 SUPERVISORY COMMITTEE	7
2.2 MONITORING AND REVIEW PROCEDURES	9
<b>3. SECTION 3 – AGREEMENT</b>	<b>10</b>
3.1 THE CONTRACT	10
3.2 WARRANTIES AND UNDERTAKINGS	10
3.3 BREACH OF THIS PROTOCOL	11
3.4 INDEMNITY AGREEMENT	12
3.5 NO THIRD PARTY RIGHTS	13
3.6 GENERAL	13
<b>APPENDIX 1 – INFORMATION SHARING PRINCIPLES</b>	<b>15</b>
<b>APPENDIX 2 – KEY LEGISLATION AND GUIDANCE</b>	<b>29</b>
<b>APPENDIX 3 – DISCLOSURE OF INFORMATION BETWEEN PERSONNEL IN DIFFERENT ORGANISATIONS</b>	<b>38</b>
<b>APPENDIX 4 – PRO FORMA FOR SUBJECT SPECIFIC INFORMATION SHARING AGREEMENT</b>	<b>50</b>
<b>APPENDIX 5 – DATA PROTECTION ACT 1998 CONDITIONS FOR PROCESSING</b>	<b>79</b>
<b>APPENDIX 6 - PARTIES TO THE AGREEMENT, ADDRESSES AND CONTACTS</b>	<b>88</b>

## **PARTIES**

This Protocol was entered into on [February 2004] and has been amended by agreement with effect from [XXXX 2005]

The parties to this Protocol (the “**Parties**”) are:

- North East London Strategic Health Authority,
- East London & The City Mental Health NHS Trust,
- Barts and The London NHS Trust,
- Homerton University Hospital NHS Foundation Trust,
- Newham Healthcare NHS Trust,
- City & Hackney Teaching PCT,
- Newham PCT (excluding host responsibilities for NHS Direct),
- Tower Hamlets PCT,
- The Corporation of London (in respect of Social Services only),
- The London Borough of Hackney (in respect of Social Services only),
- The London Borough of Newham (in respect of Social Services, Education and Housing only)
- The London Borough of Tower Hamlets (in respect of Social Services, Education and Housing only)

(whose addresses are as set out in Appendix 6 below) and any other organisations who subsequently agree to adhere to and become party to this Protocol.

## **DEFINITIONS**

In this Protocol, which for the avoidance of doubt includes its appendices, the following terms have the following meanings:

“AHRA”	the Access To Health Records Act 1990
“CDA”	the Crime and Disorder Act 1998
“CPIA”	the Criminal Procedures And Investigations Act 1996
“the Committee”	has the meaning in paragraph 2.1.1 below
“ <i>Consent to Disclosure Form</i> ”	has the meaning in paragraph 10.6 in Appendix 1
“ <i>Disclosure In Circumstances Of Risk Form</i> ”	a form conforming to Form C in Appendix 3
“ <i>Disclosure Request Form</i> ”	a form conforming to Form A in Appendix 3
“DPA 1998”	the Data Protection Act 1998
“FoIA”	Freedom Of Information Act 2000

“HSCA”	the Health and Social Care Act 2001
“HRA”	the Human Rights Act 1998
“Indemnified Party”, “Indemnifying Party” and “Indemnified Claim”	have the meanings in paragraph 3.4 below
<i>“Information Sharing Record Form”</i>	a form conforming to Form B in Appendix 3
“Joint Party Group”	a joint or interagency project or working group, or joint or interagency working arrangements
“Need to Know”	has the meaning described in paragraph 5 of Appendix 1
“personal information”	“personal data” as defined in the DPA1998
“Personnel”	the Parties’ employees, officers, elected members, directors, voluntary staff, consultants and other contractors and their sub-contractors (whether or not the arrangements with such contractors and sub-contractors are subject to legally binding contracts) and such contractors’ and their sub-contractors’ Personnel
“sensitive personal data”	has the meaning in paragraph 8 of Appendix 2
“service users”	the individuals who are recipients of the Parties’ health and care services and because service users and other individuals about whom personal information is held will be “data subjects” within the meaning of the DPA 1998, in this Protocol where the context so allows “service users” will include any such data subjects
“SSISAs”	has the meaning in paragraph 1.3.2 below

## **1. BACKGROUND AND CONTEXT**

### **1.1. Policy Context**

- 1.1.1. The aim of public policy is for citizens to receive the health and social care services that they need and that the organisation of services should not impede or debase the service provided. This requires organisations to work effectively and efficiently together to tailor services to the particular circumstances of each individual. Sharing appropriate and relevant personal information about an individual between partner organisations in a secure framework is vital to the provision of co-ordinated and seamless care to that individual.
- 1.1.2. All the Parties recognise that the initial legal responsibility for personal information resides with the organisation that first created or received it. But if personal information is shared, the responsibility extends to the recipient in the receiving organisation regardless of how transitory that storage of the personal information by the receiving organisation might be.
- 1.1.3. The aim of this Protocol is to remove any potential barriers to and uncertainty about personal information sharing at both operational and managerial levels by ensuring requirements and ethical standards are satisfied.
- 1.1.4. In order to address these responsibilities and concerns, organisations have been advised by the Department of Health and the Association of Directors of Social Services Information Management Group to establish inter-organisation protocols and contracts. These will be backed by appropriate training and procedures to ensure that personal information transfer processes work smoothly and are effectively managed.

### **1.2. Local Context**

- 1.2.1. In East London, a Caldicott Guardians Forum has been established by the Parties, which has accepted the need for a multi-organisation initiative to develop personal information sharing protocols and procedures that would be acceptable to all the Parties.
- 1.2.2. Consideration will be given at a later date to extending the use of the personal information sharing protocols and procedures to cover some or all of:
  - Other health and social care communities
  - Other borough housing and education departments – to be cascaded through relevant social services departments
  - Where appropriate - specified multi-borough and multi-agency projects and initiatives
  - NHS Direct
  - London Ambulance Service
  - Medical schools within local universities
  - Primary care contractors including GPs, pharmacists, dentists and optometrists
  - Probation
  - Police
  - Voluntary sector
  - Service users and carers
  - Agencies that represent service users
- 1.2.3. The Parties have discussed together the wider issues both in relation to the Protocol itself and to a multi-organisational process for development of protocols.

### **1.3. Scope**

#### 1.3.1. This Protocol:

- (a) forms an over-arching protocol to provide a framework for the secure and confidential sharing of personal information between the Parties on a Need to Know basis between individual Personnel in order to enable the Parties to meet the needs of communities and individuals for care, protection and support in accordance with statute and government policy;
- (b) describes roles and structures to support the exchange of personal information between the Parties;
- (c) applies to the sharing of personal information relating to service users;
- (d) covers the sharing of personal information between the Parties including (without limitation) for sharing for any of the purposes listed in paragraph 7.2 of Appendix 1;
- (e) applies to the sharing of personal information whatever the medium in which it is held and however it is transmitted;
- (f) is designed to ensure that the Parties' service users are informed of the reasons why personal information about them may need to be shared and how this sharing will be managed;
- (g) applies to the activities of the Parties' Personnel;
- (h) describes how complaints from service users relating to personal information sharing between two or more organisations will be investigated and resolved.

1.3.2. This Protocol will be supplemented by Subject Specific Information Sharing Agreements (“**SSISAs**”) addressing particular personal information sharing purposes. SSISAs will set out the detailed arrangements relevant to particular personal information sharing purposes. The Parties to this Protocol will ensure that all SSISAs, although designed to meet the needs of a particular group of local citizens, will be fully compliant and consistent with this Protocol. Unless otherwise agreed by the Committee, each SSISA shall, except in so far as not relevant to the information sharing or services to which such SSISA relates:

1.3.2.1. contain at least the elements identified in Appendix 4; and

1.3.2.2. follow the pro forma format attached at Appendix 4.

### **1.4. Legislation and Guidance**

1.4.1. The key legislation and guidance affecting the sharing and disclosure of personal information as at 31 July 2005 are set out in Appendix 2. The principles and procedures embodied in this Protocol are based upon the rights of individuals under such legislation.

## 2. INFORMATION SHARING GOVERNANCE

### 2.1. The East London Health & Social Care Information Sharing Supervisory Committee

- 2.1.1. The Parties have established the following governance procedure using a supervisory body to oversee the sharing of personal information in accordance with this Protocol. The supervisory body is called the East London Health & Social Care Information Sharing Supervisory Committee (the “**Committee**”).
- 2.1.2. Each Party shall appoint one person to represent it as a member of the Committee. Each Party shall vest its representative with the authority to speak for and validly vote on behalf of that Party. Such appointed representative shall usually be the Party’s Caldicott Guardian or data protection officer or equivalent for the time being. Parties may change their appointed representatives at any time by notification in writing to the Committee Secretary in writing.
- 2.1.3. The Committee shall appoint a Committee Secretary whose tasks shall include facilitating the activities of the Committee, being a focal point for members and the public about the activities of the Committee and ensuring that the activities of the Committee are promulgated throughout the community that the Committee serves.
- 2.1.4. The expenses of the Committee and of the Committee Secretary (including the salary and other costs of employing the Committee Secretary) shall be paid by the Parties in equal proportions unless otherwise decided by the Committee and the relevant Parties.
- 2.1.5. The Committee shall meet at least quarterly. 25% of the members’ appointed representatives being present in person or by proxy shall constitute a quorum. At least seven days’ notice in writing (which may include email) shall be given by the Committee Secretary of any meeting. The Committee may permit more than one person from a Party to attend its meetings, where such attendance might assist furthering the work of the Committee, but only one appointed representative of any Party may vote on any issue. The Committee will make decisions by a simple majority of votes cast by the appointed representatives present in person or by proxy. Proxies for representatives may be appointed by a written notice from the representative making the appointment which is produced at the meeting to which it relates and presented to the Chair of such meeting. The Chair’s decision as to the validity of proxies shall be final and binding unless he or she is manifestly acting unreasonably.
- 2.1.6. All SSISAs between any two or more Parties and changes to SSISAs shall require the approval of the Committee.
- 2.1.7. The Committee shall:
  - (a) consider representations from any Party about any aspect of personal information sharing governance, including alleged breaches of this Protocol by Parties or their Personnel, whether unintentional or deliberate;
  - (b) determine and review the levels of compliance expected using the relevant Information Governance and legal benchmarks and
  - (c) where requested by parties to SSISAs, determine how conflicts between individual SSISAs should be resolved.
- 2.1.8. The Committee shall have the power to:
  - (a) approve new Parties to this Protocol. Where new Parties are approved by majority vote of the members of the Committee present at a quorate Committee meeting in accordance with paragraph 2.1.5 above, the Chair of the meeting or any person so

authorised by the Committee may sign an adherence agreement on behalf of, and so as to bind, all existing Parties so that such new Party becomes a Party to this Protocol, such adherence agreement to be in such form as the Chair of such meeting or such authorised person may approve. Each of the Parties hereby grants the authority necessary for the Chair of such meeting and/or any other person so authorised by the Committee to sign such adherence agreement on such Party's behalf;

- (b) instruct Parties to take such actions as it determines to rectify any breach of personal information sharing governance that it, at its sole discretion, considers necessary. Such actions will include but not be limited to the right to instruct Parties to delete from their records any or all items of personal information passed to them by other Parties or amend such records; For the avoidance of doubt, although no instruction by the Committee shall override any other legal obligation of a Party, failure to comply with such an instruction may still lead to exercise of the power in paragraph 2.1.8(d) even if such failure is by reason of some other legal obligation binding upon the Party concerned.
- (c) report breaches to the Information Commissioner, such reports to be made after consultation with the Party in breach unless the Committee decides that the urgency or seriousness of the breach requires that the report should be made without consultation; and
- (d) determine that a Party should cease to be a Party to this Protocol for a specific period of time, or until such actions directed by the Committee are complied with, or permanently,

BUT temporary suspension of a Party or permanent removal of a Party from being a Party to this Protocol:

- (e) SHALL NOT OF ITSELF be a reason for a Party not to share personal information with any such suspended Party, bearing in mind the underlying importance of the health and well-being of service users and others;
- (f) shall not release or suspend such Party or any other Party from its obligations or rights under paragraph 3.4 below; and
- (g) shall not prejudice any other accrued rights or obligations of such Party or any other Party in respect of any prior breach of this Protocol.

2.1.9 Each of the Parties shall via its Caldicott Guardian:

- (a) inform the Committee Secretary about actual/potential breaches of this Protocol and/or any SSISA and any gaps and problems with the implementation of the this Protocol and/or any SSISA and related procedures which it becomes aware of; and
- (b) supply to the Committee Secretary copies of all items of information (as referred to in paragraph 8.1 of Appendix 1) produced by it for use by individuals or its Personnel in the furtherance of this Protocol.

2.1.10 The Committee shall have a duty to:

- (a) maintain records of proposals by Parties to establish SSISAs;
- (b) retain copies of all items of information produced by any Party for use by individuals or the Party's Personnel in the furtherance of personal information sharing;

- (c) maintain an information conduit between Parties and where necessary between the public and Parties, including establishing and keeping up to date a website in accordance with e-Government directions; and
- (d) maintain a channel of liaison with pan-London personal information sharing initiatives and any NHS and local authority national initiatives.

2.1.11 The Committee may provide training materials and workshops for Parties and their Personnel and common materials for service users.

## **2.2. Monitoring and review procedures**

2.2.1. This Protocol will be reviewed nine months after the first date upon which it is signed and thereafter not less frequently than annually. It will be the responsibility of the Committee to arrange such reviews.

2.2.2. Legal advice will always be sought before any major changes to this Protocol are agreed.

2.2.3. Each SSISA will set out arrangements for its review. These will include details of:

- (a) the organisations responsible for reviewing and agreeing changes to the SSISA; and
- (b) the date of an initial review and the review frequency

2.2.4. Following the introduction of this Protocol and each SSISA, their use and application will be closely monitored by the relevant Parties until the date of the first formal review.

2.2.5. The use and effectiveness of this Protocol and each SSISA will be evaluated in a number of ways:

- (a) staff in all Parties will be required to log and report Protocol and SSISA uses, together with any behaviour which they believe is not in accordance with this Protocol or any SSISA. Reports of potential and actual breaches will be a major part of the formal review process;
- (b) complaints received by Parties about personal information sharing will be analysed to determine whether they relate to a breakdown or inadequacy of this Protocol or any SSISA;
- (c) before each formal review of this Protocol or any SSISA, a survey will target all stakeholder groups. This will include service users who have given or have refused consent for the sharing of their personal information. The survey will seek to establish:
  - the ease of application of the procedures
  - the effectiveness of this Protocol or the relevant SSISA in enabling organisations to share personal information appropriately
  - difficulties encountered in applying this Protocol or the relevant SSISA
  - proposals for improving procedures
  - the contribution of this Protocol or the relevant SSISA to achieving the objectives of relevant health and social care strategies

2.2.6. Complaints shall be routed through each Party's own complaints procedure.

### **3. AGREEMENT**

#### **3.1. The Contract**

- 3.1.1. Save insofar as this Protocol is an NHS contract between any Parties who are health service bodies (“NHS contract” and “health service bodies” having the meanings in section 4 of the National Health Service and Community Care Act 1990), this Protocol (including the Appendices to it) is a legally binding contractual agreement between the Parties governed by and to be construed in accordance with English law.
- 3.1.2. Subject to paragraphs 3.1.4 and 3.1.5, any Party may cease to be a party to this Protocol by giving three months formal notice in writing to the Secretary to the Committee.
- 3.1.3. Subject to paragraphs 3.1.4 and 3.1.5, any Party will cease to be a party to this Protocol following a decision to that effect by the Committee under paragraph 2.1.8.
- 3.1.4. Whenever a Party ceases to be Party to this Protocol:
- (a) it shall not terminate such Party’s obligations and rights under paragraph 3.4; and
  - (b) it shall not prejudice any other accrued rights or obligations of such Party or any other Party in respect of any prior breach of this Protocol.
- 3.1.5. Termination or expiry of this Agreement (howsoever occasioned) shall not affect the coming into force or continuation in force of paragraph 3.4 or of any provision hereof which is expressly or by implication intended to come into or continue in force on or after such termination or expiry, nor shall it prejudice any other accrued rights or obligations of a Party in respect of any prior breach of this Protocol.

#### **3.2. Warranties and Undertakings**

- 3.2.1. Each Party warrants to the others that:

- (a) it has put in place procedures that ensure that the principles of the DPA 1998 are adhered to;
- (b) it has full power and authority to enter into and perform this Protocol and when signed on such Party’s behalf this Protocol will constitute binding obligations on such Party in accordance with this Protocol’s terms; and
- (c) its signatory identified below is duly authorised to sign this Protocol on behalf of such Party

- 3.2.2. Each Party undertakes to the others to:

- (a) implement and comply with procedures that ensure that the DPA 1998, the principles and procedures set out in this Protocol and relevant NHS and DSS guidance from time to time are adhered to within its organisation;
- (b) ensure that its Personnel adhere to the principles and procedures set out in this Protocol and with the DPA 1998;
- (c) ensure that a complaints procedure, confidentiality policy and procedures, risk assessment procedure and ‘whistle blowing’ procedure are all in place, clearly linked to this Protocol and adhered to;

- (d) ensure that all Personnel have access to appropriate training and development activities to enable them to comply with the procedures laid down in this Protocol, including for example but not limited to, the correct processes and procedures for obtaining consents from individuals and the circumstances when consent is not required;
- (e) support the implementation of the SSISAs;
- (f) ensure that SSISAs established between their organisations for the sharing of personal information relating to the service user population incorporate and are consistent with this Protocol;
- (g) provide evidence to the Committee when requested, that agreed procedures and structures have been implemented;
- (h) comply with all statutory and other legal obligations from time to time affecting the sharing of personal information; and
- (i) comply with the principles and procedures set out in Appendix 1 when sharing personal information about service users.

### **3.3. Breach Of This Protocol**

3.3.1. Breaches of this Protocol shall include but not be limited to the following:

- (a) any breach of the warranties and undertakings in paragraph 3.2;
- (b) disclosure of personal information to Personnel who do not Need to Know the personal information concerned;
- (c) inadequate security arrangements and/or the inappropriate use of such arrangements;
- (d) disregard for or breach of the procedures agreed in this Protocol or any applicable SSISA;
- (e) inappropriate or inadequate use of the procedures in this Protocol or any applicable SSISA;
- (f) failure to respond as required by this Protocol or an applicable SSISA within a reasonable time to a request for personal information from another Party;
- (g) failure to conduct a risk assessment before a disclosure without consent; and
- (h) failure to accurately record such a risk assessment.

### 3.4. Indemnity Agreement

- 3.4.1. Subject to paragraphs 3.4.3 and 3.4.4, each Party which (directly or indirectly) receives any personal information shared under this Protocol undertakes to indemnify and keep indemnified any other Party and any successor organisation of it (together the “**Indemnified Party**”) which supplies such personal information under this Protocol against all claims (whenever made) by, or on behalf of, or by a third party (for example, but without limitation, the Information Commissioner) in respect of, an individual to whom such personal information relates to the extent that such claim results from a breach of the terms of this Protocol or any SSISA by such recipient Party (the “**Indemnifying Party**”).
- 3.4.2. Subject to paragraphs 3.4.3 and 3.4.4, each Party which supplies personal information under this Protocol undertakes to indemnify and keep indemnified any other Party and any successor organisation of it (together the “**Indemnified Party**”) which (directly or indirectly) receives such personal information under this Protocol against all claims (whenever made) by, or on behalf of, or by a third party (for example, but without limitation, the Information Commissioner) in respect of, an individual to whom such personal information relates to the extent that such claim results from a breach of the terms of this Protocol or any SSISA by such supplying Party (the “**Indemnifying Party**”).
- 3.4.3. In respect of each claim by an individual to which either of the indemnities in paragraphs 3.4.1 and 3.4.2 relates (an “**Indemnified Claim**”), such claim shall be notified in writing to the Indemnifying Party within 28 days after the Indemnified Party’s Chief Executive Officer (or equivalent officer of the relevant Party) becomes aware of such claim’s existence.
- 3.4.4. The Indemnified Party undertakes and agrees that once it has received an Indemnified Claim it shall:
- (a) take all reasonable steps to mitigate the sums against which the Indemnifying Party is required to indemnify the Indemnified Party;
  - (b) make no admission of liability, compromise or agreement to or with any person or any waiver in relation to the matter which may give rise to the Indemnified Claim nor otherwise prejudice the Indemnifying Party’s position in relation to the Indemnified Claim without the prior written agreement of the Indemnifying Party unless such agreement is unreasonably withheld;
  - (c) preserve all documents, records, correspondence, accounts and other information whatsoever, which would reasonably be regarded as relevant and material or potentially material to the Indemnified Claim which it has in its possession at the date it received the Indemnified Claim or which subsequently comes into its possession. After notifying an Indemnified Claim to the Indemnifying Party, the Indemnified Party shall pass to the Indemnifying Party any particulars, documents or information which it has and any it receives from any person in connection with such matter as soon as reasonably practicable after it receives the same; and
  - (d) at the request in writing of the Indemnifying Party, take such action and make all relevant Personnel available as the Indemnifying Party may reasonably request to avoid, resist, appeal, compromise or defend any liability which is, or may become, the subject of any Indemnified Claim.
- 3.4.5. In paragraphs 3.4.1 and 3.4.2 “any claim” shall include but not be limited to the following:
- (a) any claim under or arising out of the Data Protection Act 1998;

- (b) any claim under or arising out of Article 8 in Schedule 1 to the Human Rights Act 1998;
- (c) any claim for breach of contract;
- (d) any claim for unfair dismissal;
- (e) any claim in relation to discrimination based on sex, race, disability or any other basis which is now or in the future unlawful; and
- (f) any claim under or arising out of the Employment Rights Act 1996, the Trade Union Reform and Employment Rights Act 1993 or the Trade Union and Labour Relations (Consolidation) Act 1992.

3.4.6. In this paragraph 3 unless otherwise expressly stated “**indemnify**” and “**indemnifying**” any Indemnified Party against any claim include indemnifying and keeping it harmless from and against all actions, proceedings, penalties, demands, costs, expenses, liabilities, losses or damages incurred by the Indemnified Party or any successor organisation of it as a result of any such claims.

3.4.7. The Parties are encouraged to check with their insurers concerning the indemnities in this paragraph 3.4.

### **3.5. No third party rights**

3.5.1. Each Party agrees that, save to the extent of the authority granted paragraph 2.1.8(a) above, no term of this Protocol is enforceable under the Contracts (Rights of Third Parties) Act 1999 by a person who is not a Party to this Protocol.

### **3.6. General**

3.6.1. In this Protocol:

- (a) words importing one gender shall (where appropriate) include any other gender and words importing the singular shall (where appropriate) include the plural and vice versa;
- (b) references to statutory provisions shall be construed as references to those provisions as amended or re-enacted or as their application is modified by other provisions from time to time (whether before or after the date of this Protocol) and shall include references to any provisions of which they are re-enactments (whether with or without modification) and shall also include statutory instruments or orders from time to time (whether before or after the date of this Protocol) made pursuant to them; and
- (c) unless the context otherwise requires, references to paragraphs and to appendices are to paragraphs of and appendices to this Protocol

3.6.2. No variation, waiver or modification of any of the terms of this Protocol shall be valid unless in writing and signed by or on behalf of the authorised representatives of the Parties.

3.6.3. Nothing in this Protocol shall constitute or be deemed to constitute a legal partnership between any of the Parties or any Party the agent of any other Party and none of them shall have any authority to bind the others in any way by virtue of this Protocol, save as otherwise expressly provided in this Protocol.

3.6.4. All notices to be given under this Protocol will be in writing and will be sent to the address and contact name for the recipient Party shown in Appendix 6 or any other address the relevant Party may designate by notice given in accordance with this paragraph 4.6.4 to all other

Parties. Notices may be delivered personally, by first class pre-paid letter or by fax. Notices will be deemed to have been received:

- (a) by hand delivery - at the time of delivery;
- (b) by first class post - 48 hours after the date of posting;
- (c) by fax – immediately on transmission provided a confirmatory copy is sent by first class pre-paid post or delivered by hand by the end of the next business day; and
- (d) in the case of notices of Committee meetings by email to the representatives of the Parties appointed to the Committee, such emails to be to addresses provided by such representatives to the Committee Secretary and deemed to have been received upon successful transmission

## **APPENDIX 1**

### **INFORMATION SHARING PRINCIPLES**

(NOTE: The law in this Appendix is stated as at 31 July 2005)

#### **CONTENTS**

	Page
1. General Principles	16
2. Individuals' Rights Of Access	17
3. Complaints	17
4. Access And Security Procedures	18
5. Access To Personal Information – The “Need To Know”	19
6. Tracking Information	20
7. Purposes For Which Personal Information May Be Shared	20
8. Essential Information For The Citizen	21
9. The Process Of Information Exchange Between Personnel In Different Organisations: Requirement For An Audit Trail	21
10. Obtaining And Recording Consent	23
11. Capacity To Give Informed Consent	25
12. Checking For Consent Before Disclosing Personal Information	26
13. Disclosing Personal Information Without Consent	26

**1. General Principles**

- 1.1. The Parties recognise that many multi-agency services cannot be effectively delivered without the exchange of personal information and so agree to exchange, in a manner which is compliant with their legal responsibilities, personal information about individual service users, levels of activity relating to the service users and the level and nature of resources deployed in support of the service users.
- 1.2. The Parties agree to ensure that requests for personal information from each other and other NHS organisations and Social Services departments are dealt with in a manner compatible with the Caldicott Principles, the DPA 1998 and all other relevant law.
- 1.3. Personal information will be deemed to have been provided in confidence when it appears reasonable to assume that the provider of the information believed that this would be the case. It is generally accepted that most (if not all) personal information provided by service users to social care and health organisations is confidential in nature. Personal information passed between the Parties is deemed provided in confidence unless it is specifically stated that the personal information was provided by the service user on the basis that it need not remain confidential. All the Parties accept this duty of confidentiality and will not disclose such confidential personal information without the consent of the person concerned, unless there are statutory grounds and other demonstrable overriding justifications for so doing. When requesting release and disclosure of personal information from any other Party, Personnel in all Parties will respect this responsibility and not seek to override the procedures which each Party has in place to ensure that personal information is not disclosed unlawfully or inappropriately.
- 1.4. All the Parties recognise that the initial legal responsibility for personal information resides with the organisation that first created or received it. But if personal information is shared, the responsibility extends to the recipient in the receiving organisation regardless of how transitory that storage of the personal information by the receiving organisation might be.
- 1.5. The requesting Party will only ask for information that it has a Need to Know. ("Need to Know" is defined in paragraph 5 of this Appendix.)
- 1.6. Each Party shall ensure that personal information shared with it by another Party will not be disclosed by it to any other person unless:
  - (a) that recipient has a Need to Know such information; and EITHER
  - (b) the individual to whom the personal information relates has consented to such disclosure and the purposes for which the recipient will use the personal information;  
OR
  - (c) such disclosure is otherwise permitted by law.
- 1.7. Save in the case of limited exceptions, personal information shared with Personnel of another Party for a specific purpose should not be treated by the receiving Party as intelligence for the general use of the organisation or used or disclosed except in support of a purpose for which it was first collected.
- 1.8. Though information about a deceased person is not caught by the DPA 1998, confidential information about a deceased person will remain subject to the duty of confidence. Therefore, careful consideration will be given to the disclosure of such confidential information concerning a deceased person and, if necessary, legal advice will be sought on individual

cases.

## **2. Individuals' Rights of Access**

- 2.1. The Parties will comply with the rights of individuals under the DPA 1998 to be informed about personal information that is recorded about them, including the rights described in paragraph 11 of Appendix 2.
- 2.2. Where there is a joint record containing personal information all the joint holders must have arrangements in place to provide access.
- 2.3. Unless statutory grounds exist for restricting an individual's access to personal information relating to him or her, an individual will be given every opportunity to gain access to personal information held about him or her and to correct any factual errors that have been made. Similarly, where an opinion about a service user has been recorded and the service user feels this opinion is based on incorrect factual personal information, the service user will be given every opportunity to correct the factual error and record his or her disagreement with the recorded opinion.
- 2.4. The existing statutory grounds exist for restricting an individual's access to personal information relating to him or her include the orders under Section 30 of the DPA 1998 in relation to access to some health, education and social work circumstances. Parties shall ensure that their Personnel understand and comply with these statutory orders which are described in part 3 of Appendix 5.
- 2.5. If a Party has statutory grounds for restricting an individual's access to personal information relating to him or her following a request, then the individual will be told that such personal information is held and on what grounds it is restricted unless it is apparent there is a risk that to do so would put the individual or some other person at risk.
- 2.6. Where a member of a Party's Personnel or any other person (whether or not a service user) requests that personal information supplied by them about an individual be kept confidential from that individual, under the DPA 1998 that will not necessarily be grounds for refusing disclosure to the individual. Therefore, the outcome of this request and the reasons for taking the decision whether or not to disclose it to the individual concerned under the DPA 1998 will be recorded in the individual's service user record. The decision by an organisation to keep personal information confidential from the individual will only be taken in compliance with the DPA 1998.
- 2.7. Each Party will ensure that:
  - (a) all its Personnel are aware of, and comply with, their responsibilities in regard both to the confidentiality of personal information about service users and other people who are in contact with their organisation and to the commitment of that Party to share personal information; and
  - (b) all new and temporary Personnel will be appropriately briefed on their responsibilities as part of their induction process.

## **3. Complaints**

- 3.1. The Parties confirm to each other that:
  - (a) they have put in place efficient and effective procedures to address complaints relating to the disclosure of personal information, and service users will be provided with information about these procedures;

- (b) they will keep a record of all such complaints received; and
- (c) they have established a procedure by which their complaints officers report complaints regarding the inappropriate use or disclosure of personal information to **the Caldicott Guardian or data protection officer** or equivalent

#### **4. Access And Security Procedures**

- 4.1. It is essential that requests for sharing of personal information about particular individuals be accompanied by sufficient personal information to ensure that the person can be clearly identified.
- 4.2. In the absence of an applicable common identifier (e.g. NHS number, where applicable), the name, address and date of birth of the individual should accompany requests for personal information wherever possible.
- 4.3. The Parties will take every reasonable precaution to ensure that personal information that identifies individual service users is transferred and shared in as secure manner as practicable.
- 4.4. The Parties will comply with any mechanisms introduced with the prior approval of the Information Commissioner for anonymity of information held in the NHS Care Records Service.
- 4.5. Electronic transfer of personal information (other than by email) will only be permitted on a person to person basis across secure networks or by disk (with the personal information protected by password) or other digital device (again with the personal information protected by password) addressed or delivered directly to the intended recipient. The passwords should be issued separately, or via telephone once information is received. Fax transfer should be avoided wherever possible but where used shall be conducted through "safe havens" (namely fax machines designated under the recipient Party's procedures as "safe haven" fax machines) with immediate collection and receipt confirmed.
- 4.6. Save as varied under an SSISA with the prior agreement of the Committee, where email is used for transfer of personal information an approved encryption method should be applied. Co-signatories will move to these approved standards but it is recognised this will take time. In the interim, where an encrypted Email service cannot be used, additional protection (e.g. passwords) and/or anonymisation of information should be used. Passwords will be issued separately, or via telephone once information is confirmed as received by the intended recipient
- 4.7. Where messages referring to identifiable individuals are sent by email or electronic transfer systems, unless the email or electronic transfer systems are within the relevant Party's formal record-keeping systems subject to security procedures and protections complying with the DPA 1998, such messages should not be stored on email or electronic transfer systems, but the personal information should be printed off and filed and the original message deleted.
- 4.8. The above requirements (which may be covered in individual SSISAs) apply equally to the use of mobile devices such as Pocket PCs, personal digital assistants (PDA's), telephones, bleeps and air-calls and the services they provide (e.g. "texting").
- 4.9. It is recognised by the Parties that in urgent cases, personal information about individual service users may have to be requested or provided by telephone or verbally face to face. Non-urgent requests in cases covered by a SSISA may also be requested or provided by telephone or verbally face to face. No identifiable patient information shall be given to an

unrecognised or an unverified person over the telephone. All requests for information taken over the telephone must be recorded and logged. Personnel receiving a telephone request for personal information sharing should always call the requesting person back to check identity before releasing personal information over the telephone

- 4.10. Written communications containing personal information should be transferred in sealed envelopes (plain rather than internal office transit envelopes) and addressed by name to the intended recipient within the relevant organisation. They should be marked "Private and Confidential – to be opened by the recipient only" and (if very heavy) double wrapped or sent by recorded delivery. The intended recipients should be alerted to the despatch of such personal information and should make arrangements within their own organisations to ensure both that the envelopes are delivered to them unopened and that they are received within the expected timescale.
- 4.11. Where a Party has a policy that all mail is to be opened at a central point, prior to delivery to the named recipient, then this policy must be made clear to all Parties so that alternative means of transfer may be adopted to ensure that the personal information is restricted to those who have a Need to Know.

## **5. Access to Personal Information – the "Need to Know"**

- 5.1. Where it is necessary for personal information to be shared, personal information will be shared on a need-to-know basis only. The Parties will put measures in place to ensure that access is restricted to those who "Need to Know" and will monitor compliance.
- 5.2. The Need to Know requirement means that Personnel will only have access to personal information if it is lawful for such Personnel to have access to such personal information for the relevant purpose and the function they are required to fulfill at that particular time, in relation to a particular service user, cannot be achieved without access to the personal information specified.
- 5.3. Access to electronic systems will be defined by Personnel role and the Need to Know specific elements of personal information. Menus will be defined for various Personnel roles and access provided accordingly.
- 5.4. Depending on the level of consent given by the service user to sharing specific elements of personal information which is sensitive personal data in electronic systems, it may be necessary only to allow access to this data to team managers or other designated senior Personnel.
- 5.5. Where personal information is contained in manual or paper files, special procedures will be applied to control access. These will include rules about where any sensitive personal data is recorded and stored. It may be stored separately, and subject to more stringent access rules.
- 5.6. Each Party will conduct regular auditing of its "Need to Know" principles and practices and breaches may be subject to disciplinary proceedings.
- 5.7. Each Party shall implement and maintain procedures for recording, and alerting its Personnel to, any request or requirement imposed by an individual that personal information about him or her shall not be shared with any particular person or class or classes of person.
- 5.8. In addition to the Parties' obligations concerning contractors under Principle 7 of the DPA 1998, each Party will ensure that it has a written agreement with its contractors and require that its contractors impose written agreements on their sub-contractors which requires the contractors and sub-contractors to have in place procedures consistent with and complying with this Protocol and any applicable SSISA.

## 6. Tracking Information

- 6.1. Compliance with the Caldicott Principles requires that each Party is able to map and track personal information streams flowing in and out of it.
- 6.2. The Parties undertake to establish an audit trail by recording in the service user's record what was disclosed in each case **by whom, when** and for **what purpose**. If disclosure is made other than in accordance with the terms of this Protocol, the authority that permitted the disclosure must be recorded.
- 6.3. The Party which discloses information to another Party shall have no obligation under this Protocol to notify the recipient Party of any changes to such information. This does not preclude an SSISA between such Parties or other agreement between them imposing express obligations to update information disclosed.

## 7. Purposes for which personal information may be shared

- 7.1. The disclosure of personal information to another organisation by a data controller amounts to processing under the DPA 1998.
- 7.2. This Protocol applies to the sharing of personal information between the Parties, including without limitation sharing for the following purposes:
  - (a) improving the health of service users;
  - (b) protecting people and communities;
  - (c) supporting people in need; and
  - (d) investigating complaints
- 7.3. Personal information may be shared for the purposes listed below but in each of these cases the Parties undertake that the disclosing Party shall (unless necessary in the circumstances and permitted by law) anonymise the personal information by stripping those personal information of all personal identifiers before disclosing it, so that the person to whom it applies cannot be identified from the information disclosed even if combined with other information that the recipient has or is likely to come into the possession of. The purposes to which this paragraph 7.3 relates are:
  - (a) managing & planning services;
  - (b) commissioning and contracting services;
  - (c) developing inter-organisational strategies;
  - (d) performance management and audit; and
  - (e) research.
- 7.4. The duty of confidentiality requires that personal information that has been provided in confidence should only be used for the purposes that the individual has agreed to. This duty can only be overridden when there is a clear statutory requirement or permission to do so or the holder of the personal information can justify disclosure as being in the public interest (e.g. to protect others from harm).

- 7.5. In addition to ensuring that there is an appropriate justification for any sharing without consent, the Parties will also check that there are no statutory restrictions on the particular sharing envisaged. To this end, each Party shall maintain an up to date list available to its Personnel describing the statutory restrictions that may be relevant to its area of activity.
- 7.6. Each Party shall make notifications to the Office of the Information Commissioner as required by the Part III of the DPA 1998. Each Party shall ensure that such notifications include notification that such Party may disclose personal information to other persons (who may or may not be Parties) in circumstances of risk of harm to individuals.

## **8. Essential Information For The Citizen**

- 8.1. In order to ensure that consent to the sharing of personal information is 'informed', all Parties confirm that they have available to members of the public material which explains:
- (a) the rights of individuals under the DPA 1998, particularly in relation to sensitive personal data;
  - (b) details of the procedures in place to enable service users to access their records;
  - (c) details of the procedures which may have to be initiated when a member of Personnel suspects that a service user has been or is at risk of abuse for example under a 'Service User Protection Policy' or 'Mental Health Risk Assessment & Management Policy'. Such policies will explain in general terms to whom the personal information will be shared at differing stages, as well as what personal information will be shared and how it will be used;
  - (d) details of the circumstances under which personal information may be shared without consent and the procedures that will be followed;
  - (e) details of the complaints procedures to follow in the event that the individual concerned believes personal information about him or her has been inappropriately disclosed;
  - (f) details of how the personal information individuals provide will be recorded, stored and the length of time it will be retained both by the originating organisation and the organisations to whom they may disclose that personal information; and
  - (g) details of the length of time for which consent to particular disclosures is valid, for example in the case of adoption 75 years.
- 8.2. The above leaflets will be made available to individual service users even in routine episodes of care and treatment All of the above leaflets will be referenced on each Party's website and on the Committee's Information Governance website. The above information will be available in a variety of languages and formats where reasonable to reflect the ethnic composition of each of the boroughs within the local health/care community.

## **9. The Process of Information Exchange Between Personnel In Different Organisations: Requirement For An Audit Trail**

- 9.1. Personal information exchange between organisations and Personnel in different organisations takes place in a number of ways (for example, sometimes the sharing will be initiated by the disclosing Party and there will be no request for it). It is not reasonable to expect **all** such sharing of personal information to be formally sanctioned via paper-based requests, because this could significantly interrupt the 'flow' of care or potentially compromise the ability of Personnel to intervene swiftly at times of risk.

- 9.2. Nonetheless, it will be the responsibility of all Parties to maintain an audit trail of personal information disclosed and received in the course of information sharing to which this Protocol relates. Where Parties exchange personal information under an SSISA which sets out the procedure for maintaining the audit trail, the Parties shall follow the SSISA's procedure.
- 9.3. Where an SSISA is entered into for a Joint Party Group, the Parties concerned may provide in the relevant SSISA for the audit trail into and out of the Joint Party Group, but otherwise the audit trail shall be maintained through the record keeping of the Joint Party Group.
- 9.4. The following provisions of this paragraph 9 are subject to variation in SSISAs.
- 9.5. In circumstances not covered by an SSISA, and where there is no obvious issue of risk (and so no urgency for the request), it is recommended that a Party requesting should make a written request for sharing of the information (for example by completing and supplying a *Disclosure Request Form*, although use of that precise form is not mandatory) and if it does not do so, some other reasonable method should be used for both the Parties concerned to maintain the audit trail. When making the request the Personnel requesting the personal information shall give clear and specific guidance about the nature of the personal information requested, the purpose for which the personal information will be used.
- 9.6. Since much personal information exchange occurs via electronic means, the Parties undertake to each other to have an on-line *Disclosure Request Form* available to download within each organisation. If this is completed and sent by e-mail, then the recipient can respond by return if needed. The completed form must be printed, and promptly placed on the service user's files held by both the requesting Party and the disclosing Party as a formal record of the request.
- 9.7. Where personal information is requested verbally and outside the procedures covered by an SSISA, for example as part of a risk assessment process, Personnel may delay completion of a written record until **after** the personal information has been shared.
- 9.8. Records of requests for personal information sharing (in whatever form) will need to be promptly placed on the service user's files held by both the requesting Party and the disclosing Party as a formal record of the request.
- 9.9. Where sharing of personal information is initiated by the disclosing Party and there is no request for it there will be no *Disclosure Request Form*. A Party should not initiate sharing of information to another Party without a request unless:
  - (a) that recipient has a Need to Know such information; and EITHER
  - (b) the individual to whom the personal information relates has consented to such disclosure and the purposes for which the recipient will use the personal information;  
OR
  - (c) such disclosure is:
    - is necessary and permitted by law in "circumstances of risk" (see paragraph 13 of this Appendix 1) to any person; or
    - is required by law.
- 9.10. When Personnel disclose personal information to another Party (whether or not in response to a request) and do so outside the record keeping procedures covered by an SSISA, it is

recommended that the Party sharing the personal information should make a written record that the information was shared (for example by completing and supplying an *Information Sharing Record Form*, although use of that precise form is not mandatory) and if it does not do so, then some other reasonable method should be used for the disclosing Party to maintain the audit trail. The audit trail record must briefly identify the personal information shared and the purpose for which it was shared.

- 9.11. Records recording sharing of personal information (in whatever form) will need to be placed on the service user's file held by the disclosing Party as a formal record of the sharing.
- 9.12. When disclosing personal information about individuals, Personnel shall clearly state whether the personal information being supplied is fact or opinion, or a combination of the two.
- 9.13. Save that the Parties agree that it should only take place on a Need to Know basis, the internal disclosure of personal information amongst Personnel within the same Party for the purpose of delivering care to the service user will not be information sharing to which this Protocol relates. The Parties confirm to each other that such processing can be tracked through their normal service user record management.

## 10. Obtaining and Recording Consent

- 10.1. Consent to personal information sharing will be sought from all service users, normally at the first contact with the person concerned unless the individual is unable, at that time, to fully comprehend the implications or make an informed judgement. The Personnel who seek consents from individuals will have been trained in the correct processes and procedures.
- 10.2. In seeking consent to disclose personal information, organisations will ensure that:
  - (a) the consent is a "freely given informed indication of the individual's wishes";
  - (b) the individual understands the purposes for which it will be used;
  - (c) the individual is made aware of the Party with which the personal information may be shared; and
  - (d) consent will not be treated as having been given either by the individual or his or her representative, unless it has been made clear to them what the implications of such consent will be.
- 10.3. Where Parties obtain personal information about an individual which is "sensitive personal data" as defined in the DPA 1998 (see paragraph 8 of Appendix 2 for the definition) in the course of their direct contact with that individual, they shall whenever it is, or may be, appropriate for a specific purpose seek to obtain the **Explicit Consent** of that individual to disclose that personal information to any other Party or any other body for such purpose. If such consent is not given, because the individual is either unable or unwilling to give that consent, then that sensitive personal data will only be released to another Party if there are grounds for overriding the duty of confidence (see paragraph 13 of this Appendix) and one of the remaining conditions of Schedule 3 of the DPA can be demonstrated or one of the few circumstances where there is an applicable statutory exemption can be demonstrated. The provisions of Schedule 3 and applicable statutory exemptions are described in Part 2 of Appendix 5.
- 10.4. "**Explicit Consent**" means that the consent should be absolutely clear and in appropriate cases it should cover the specific detail of the processing, the particular type of personal information to be processed (or even the specific personal information), the purposes of the

processing and any special aspects of the processing which may affect the individual, for example, disclosures which may be made of the personal information.

- 10.5. The Parties each confirm that they have in place a “**consent recording policy**” that is monitored, and supports compliance with the DPA 1998.
- 10.6. To the extent appropriate consent for sharing personal information has not already been obtained under the relevant Party’s consent recording policy, the party will obtain any necessary consent from service users, using a consent to disclosure form (“*Consent to Disclosure Form*”). Parties may prepare their own *Consent to Disclosure Forms* but they must contain at least the information in Form D in Appendix 3. *Consent to Disclosure Forms* must be completed and signed by either the service user or his or her legally authorised representative and shall detail the restrictions (if any) to be placed upon the disclosure of personal information.
- 10.7. Completed *Consent to Disclosure Forms* shall be placed in an easy to find, accessible place within the service user’s file, all clearly date marked, because individuals have the right to change their minds about consent in the future.
- 10.8. A copy of the completed *Consent to Disclosure Form* should be given to either the service user, or his or her legally authorised representative, and must be dated and signed by a member of Personnel, the service user, and/or his or her legally authorised representative.
- 10.9. The Parties agree that, subject to certain statutory exceptions, an individual has the right to limit:
  - (a) the ways in which the Party first receiving or generating personal information
    - can share personal information with other organisations
    - can disclose what can be shared, and what remains confidential
  - (b) the specific purposes in which confidential personal information might be disclosed,and has a right to redress if personal information about the individual has been unlawfully disclosed
- 10.10. Where a service user declines consent to disclosure and/or changes the extent of consent, and/or the nature of a requested disclosure is problematic, then guidance must be sought from the individual or (where appropriate) his or her legally authorised representative, if any and he or she should be informed in a sensitive manner where the lack of consent may place a limitation on the provision of specific services and why the specific information is required for the provision of that service. In the absence of the individual or (where appropriate) his or her legally authorised representative, then Personnel must, where practicable:
  - (a) discuss the situation with the Caldicott Guardian or equivalent officer within the Party, and take guidance from him/her on the best way in which to proceed;
  - (b) undertake a risk assessment to establish whether withdrawal of consent to disclose personal information might result in significant harm to the individual or others. This must be written-up, and dated and signed;
  - (c) evidence of significant risk based on professional judgement may be sufficient to override the wishes of the person deemed to be at actual/potential risk; and
  - (d) consider whether there are legal bases which permit disclosing without consent (for example, under the DPA 1998, the HRA and exceptions to the duty of confidentiality).

## 11. Capacity To Give Informed Consent

- 11.1. Individuals are only able to give informed consent if they have the cognitive ability to do so, and in some instances, this ability might be intermittent, e.g. where adults and older people have certain forms of dementia, individuals with learning disabilities, and adults with particular forms of mental illness. A significant number of the Parties' health and care service users will be unable to give informed consent, or are unable to do so consistently.
- 11.2. The capacity to give consent can be assessed by considering whether the individual:
- (a) has the capacity to make this particular decision;
  - (b) has the capacity to understand and retain the information relevant to the decision;
  - (c) will be able to understand the reasonably foreseeable consequences of deciding one way or the other; and
  - (d) will have the capacity to communicate the decision he or she has come to
- 11.3. If it is proposed to share personal information in respect of a **child under 16**, a judgement needs to be made in each case as to whether the child understands the nature of the request and therefore has the capacity to give consent. Where a judgement is needed it is good practice to encourage the child to involve his or her parent (or other person with "parental responsibility") in the decision making. If it is felt that the child is unable to understand, then consent must be sought from the parent or other person with "parental responsibility".
- 11.4. **Adults** (including for this purpose **young people aged 16-17**) are always assumed to be competent to give consent unless it is demonstrated otherwise. If there is doubt about capacity this should be considered in relation to the criteria listed in paragraph 11.2 above.
- 11.5. If an adult (including for this purpose a **young person aged 16-17**) service user is unable to give informed consent then decisions to disclose information will generally be taken by the Personnel concerned, unless another person has the legal authority to take decisions on the service user's behalf. Any decision will take into account the service user's best interests and the views of relatives or carers. A service user's previous refusal (given while the service user had capacity to decide) to particular information being passed on will normally be regarded as decisive.
- 11.6. Where a service user's "capacity" may change from day to day (for example as a consequence of fluctuating mental health), a decision on consent will be deferred wherever possible, until such time as the service user is able to be involved in the decision making process. In such circumstances:
- (a) Personnel working in such situations should still advise the service user (if possible in the presence of a representative or advocate) what personal information needs to be shared, with whom, and for what purpose;
  - (b) a time frame in which the Party wishes to receive formal consent needs to be given to the service user;
  - (c) this discussion should be clearly recorded in the service user's contemporaneous notes; and
  - (d) the Caldicott Guardian of the organisation should be advised in writing if the supervisor

of the relevant Personnel feels it to be appropriate and will be informed if consent is not obtained within the stated timeframe.

- 11.7. Where it is considered that a service user does not have capacity, a record will be made of this decision and the steps taken by the Personnel concerned to reach a decision about whether personal information should be shared.
- 11.8. The Parties undertake to each other to ensure that their own Personnel are aware that informal carers or advocates that do not have the necessary legal authority are NOT ABLE to provide consent on behalf of another person.

## **12. Checking for Consent Before Disclosing Personal Information**

- 12.1. Each of the Parties will ensure that before disclosing personal information its Personnel will follow the procedure below:
  - (a) always check the service user file for the most recent *Consent to Disclosure Form*;
  - (b) if practical (and it will be easier if the service user is present), check with the service user the detail of the form, to ensure that it is still relevant to the present circumstances and appropriate to the episode of care or treatment (for example some alteration may be required because of the passing of time or changed circumstances);
  - (c) any significant change will warrant the completion of a new *Consent to Disclosure Form*, which must be clearly date marked and signed by the member of Personnel, the service user and/or his or her legally authorised representative; and
  - (d) if the discussion about consent suggests that the service user's capacity to give informed consent is declining, Personnel should refer to paragraph 11 of this Appendix.

## **13. Disclosing Personal Information Without Consent**

- 13.1. Disclosure of personal information without the informed consent of the individual concerned can lead to disciplinary action, civil legal action or even prosecution of Personnel of public sector organisations, and to the prosecution of the organisations themselves.
- 13.2. Disclosure of personal information without consent must be justifiable under both:
  - (a) one of the conditions in Schedule 2 of the DPA 1998 (these conditions are listed in Part 1 of Appendix 5); and
  - (b) an exception to the duty of confidentiality,and in addition, if the personal data is "sensitive personal data" and there is no "Explicit Consent",
  - (c) at least one of the conditions of Schedule 3 of the DPA 1998 or another exemption will need to apply. These conditions and exemptions are listed in Part 2 of Appendix 5.
- 13.3. Practical examples of where the exemptions apply include:
  - (a) where there is a statutory duty upon a clinician to communicate the information (such as statutory notification of certain infectious diseases);
  - (b) where release of the information is required by a court order; or

- (c) where release of the information is considered to be in the public interest (such as notification of an uncontrolled epileptic who continues to drive a car). It is not always easy to decide whether the public interest is strong enough to override a common law duty of confidentiality and Parties and their Personnel should take legal advice if there is any doubt. The need to safeguard the interests of the service user and any other person to whom the personal information relates will be a key consideration.
- 13.4. Even where the restrictions imposed by the DPA 1998 are satisfied, disclosure of personal information without consent will be limited to situations where professional judgement concludes that a risk situation exists and the duty of confidentiality can be overridden. The Parties recognise that the 'risk assessment' process can only indicate the probability of a particular outcome arising based upon the gathering of available personal information. Where serious concerns exist, Personnel must discharge their statutory duties.
- 13.5. Examples of a clear overriding public interest displacing the duty of confidentiality are where there is a risk to the life of a child or a risk that a child will be seriously injured. Less clear cut situations include where there is a matter of "real public concern" or where a Party wants to make the information available to promote another public purpose. A matter of "real public concern" can include the prevention of crime or a breach of national security. Express statutory powers may also permit disclosure of the information in this sort of situation. One public body can sometimes justify disclosure of information that is subject to a duty of confidentiality to assist another public body in performing its public functions. However, the application of this defence is limited, and legal advice should be sought as to its relevance in every particular case.
- 13.6. In deciding whether or not disclosure of information given in confidence is justified, Parties and their Personnel need to weigh the harm that would result from breach of confidence against the harm that might result if they fail to disclose the information. Disclosure cannot be justified simply because a competing public interest exists. The disclosure must be proportionate and the minimum necessary to achieve the public interest objective.
- 13.7. The Parties undertake to abide by the following procedure:
- (a) where a member of Personnel has serious concerns about the immediate health and well being of an individual, or others that might come into contact with that person, then guidance on sharing personal information with another organisation without the individual's consent must be sought in the first instance from a line manager;
- (b) where the risks to the individual or another person are considered so great, and/or the individual is either unwilling or unable to give consent to disclosure, then the member of Personnel or line manager, acting in good faith, should disclose this personal information to the relevant organisations immediately. Failure to do so might be viewed as failure of the organisation that is aware of the risk to discharge its duty of care, particularly if there is resultant harm; and
- (c) should the risks be viewed more as 'concerns' that might constitute future 'risk', then the member of the Party's Personnel will advise a line manager, and then complete a *Disclosure In Circumstances Of Risk Form* or in any other written form which contains all the information required in Form C in Appendix 3. This may involve a further attempt to seek the consent from the service user. If the service user continues to refuse to agree to the sharing of this personal information, the member of the Party's Personnel must consult a line manager who may authorise the member of Personnel to proceed with the sharing of information after completing the 'Risk Assessment' section of the form to record concerns and justify the disclosure of personal information without informed consent of the individual concerned. There must always

be a fully documented 'Risk Assessment' section attached to the *Disclosure In Circumstances Of Risk Form* where disclosure without consent is occurring "in circumstances of risk".

- 13.8. The Parties confirm to each other that they have put in place procedures to ensure that decisions to disclose personal information without consent are made only after full consideration of the obligations of confidentiality and the relevant applicable legislation (including Schedule 2 and, in the case of sensitive personal data, Schedule 3 of the DPA 1998) and that these decisions can be audited and defended. The Parties undertake to each other to ensure that:
- (a) all their Personnel that may be involved in making such decisions have been provided with training in these procedures and all new Personnel will be provided with such training before being permitted to make such decisions;
  - (b) all their Personnel will be made aware that disclosure of any personal information to another person, which cannot be legally justified, whether the disclosure was inadvertent or intentional, will be subject to disciplinary action; and
  - (c) a record is made and retained of all known incidents of unlawful disclosure that occur.

## **APPENDIX 2**

### **KEY LEGISLATION AND COMMON LAW**

#### **CONTENTS**

The Data Protection Act 1998 (“DPA 1998”)	30
The Common Law Duty of Confidentiality	34
The Caldicott Principles	34
The Human Rights Act 1998 (“HRA”)	35
The Access to Health Records Act 1990 (“AHRA”)	35
Freedom of Information Act 2000 (“FoIA”)	35
The Crime and Disorder Act 1998 (“CDA”)	36
The Criminal Procedures and Investigations Act 1996 (“CPIA”)	36
Regulation of Investigatory Powers Act 2000	36
Health and Social Care Act 2001 (“HSCA”)	36

## Introduction

From a practical point of view, the two most relevant elements of the legal framework governing information sharing are the Data Protection Act 1998 and the common law duty of confidentiality, each of which must be viewed in the light of the Human Rights Act 1998

(NOTE: The law in this Appendix is stated as at 31 July 2005)

### The Data Protection Act 1998 (“DPA 1998”)

1. Since 1 March 2000 the DPA 1998 has been the key legislation governing the protection and use of personal information about identifiable individuals (referred to as “**Personal Data**” in the DPA 1998). The DPA 1998 was passed in response to the EU Data Protection Directive (95/46/EC). Compliance with the DPA 1998 should ensure that when personal information is used or disclosed, it is done safely and with regard to the rights of the individual concerned. The DPA 1998 does not apply to information relating to the deceased (see paragraphs 18 and 26 of this Appendix).
2. The personal information falling within the meaning of “Personal Data” includes expressions of opinion about individuals and indications of intentions of persons in relation to individuals. The DPA 1998 applies to manual and electronic records. For some categories of manual personal information there are exemptions from some aspects of the DPA 1998 up to 24 October 2007.
3. The DPA 1998 gives seven rights to individuals in respect of their own personal information held by others. They are:
  - (a) the right of subject access;
  - (b) the right to prevent processing likely to cause unwarranted, substantial damage or distress;
  - (c) the right to prevent processing for the purposes of direct marketing;
  - (d) rights in relation to automated decision taking;
  - (e) the right to take action for compensation if the individual suffers damage;
  - (f) the right to take action to rectify, block, erase or destroy inaccurate personal information; and
  - (g) the right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the DPA 1998 has been contravened.
4. The “processing” of personal information by “**data controllers**” (i.e. the person or organisation that alone or jointly with others determines the purposes for which, and the manner in which, personal information is processed) is regulated by eight Data Protection Principles. “**Processing**” is defined very broadly and encompasses more or less anything that might be done with personal information, including just holding it. The eight Data Protection Principles are:
  - (a) personal information shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- (subject to limited exemptions) the “fair processing code” information has been supplied – see paragraph 5 of this Appendix
  - at least one of the conditions in Schedule 2 of the DPA 1998 is met; and
  - in the case of personal information which is “sensitive personal data” (see paragraph 8 of this Appendix), at least one of the conditions in Schedule 3 of the DPA 1998 is also met.
- (b) personal information 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.
- (c) personal information shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
- (d) personal information shall be accurate and, where necessary, kept up to date.
- (e) personal information processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or purposes.
- (f) personal information shall be processed in accordance with the rights of individuals under the DPA 1998.
- (g) appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information.
- (h) personal information shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal information.
5. The “**fair processing code**” (imposed by Schedule 1 of the DPA 1998) requires that when obtaining personal information from an individual a data controller must inform the individual of:
- (a) the identity of the data controller;
  - (b) any nominated representative of the data controller for the purposes of the DPA 1998;
  - (c) the purposes for which the personal information is intended to be processed; and
  - (d) any further information which is necessary to enable the processing to be fair having regard to the specific circumstances of the intended processing (e.g. who it may be disclosed to)
6. Schedule 2 of the DPA 1998 is a list of conditions set out in Part 1 of Appendix 5 to this Protocol, at least one of which must be met before personal information can be processed fairly and lawfully.
7. The DPA 1998 defines “**sensitive personal data**” as personal information which relates to:
- (a) the individual’s racial or ethnic origin;

- (b) the individual's political opinions;
  - (c) the individual's religious beliefs or other beliefs of a similar nature;
  - (d) whether the individual is a member of a trade union;
  - (e) the individual's physical or mental health or condition;
  - (f) the individual's sexual life;
  - (g) the commission or alleged commission by the individual of any offence; or
  - (h) any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings.
8. Schedule 3 of the DPA 1998 provides an additional list of conditions for processing **sensitive personal data** fairly and lawfully. Unless an exemption applies, the individual must give his or her explicit consent or one of the other conditions must be met. These conditions and exemptions are summarised in Part 2 of Appendix 5 to this Protocol but, importantly, they contain a medical purposes condition allowing processing without consent.
9. Processing must be lawful. The DPA 1998 does not provide any guidance on the meaning of "lawful" but "unlawful" has been defined by the Courts as "something which is contrary to some law or enactment or is done without lawful justification or excuse". The term applies equally to the public and private sectors and to breaches of both statute and common law, whether criminal or civil. This means that a data controller must comply with all relevant rules of law whether derived from statute or common law, relating to the purpose and ways in which the data controller processes personal information. Examples of information unlawfully obtained might be information, which is obtained as a result of a breach of confidence or in breach of an enforceable contractual agreement. An example under statute is that legislation specifically precludes council tax information being used for other purposes, so consent would not be enough. Similarly use of personal information by a public authority in breach of the limits on its statutory powers (i.e. acting "ultra vires") or its delegated powers is unlawful.
10. Nonetheless, even where the Schedule 2 and 3 conditions in the DPA 1998 are satisfied, that alone may not permit disclosure. However, there are circumstances where organisations would still be able to make a disclosure. For example:
- (a) Section 29 of the DPA 1998 provides an exemption from compliance with:
    - the first data protection principle (apart from the need for satisfaction of the Schedule 2 and 3 conditions) – so, where section 29 applies the obligation to tell individuals about the disclosure is removed;
    - the second, third, fourth and fifth data protection principles; and
    - the subject access obligations (described in paragraph 11 below)to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders or the assessment or collection of any tax or duty or similar, and where those purposes by non-disclosure. Section 29 does not override common law obligations of confidentiality, but see sub-paragraph (c) below;
  - (b) disclosure without consent is also permitted where disclosure is required by law;

- (c) for the purposes of the common law duty of confidentiality, if there is no consent, the individual's right to confidentiality would need to be balanced against countervailing public interests - again preventing crime is accepted as one of those interests where the offence is sufficiently serious that the public interest overrides. The rights in Article 8 in the Human Rights Act 1998 would also need to be considered.
11. As mentioned in paragraph 3 of this Appendix, individuals have rights of access to personal information about themselves. An individual is entitled:
- (a) to be informed by any data controller whether personal information about that individual is being processed by or on behalf of that data controller;
- (b) if that is the case, to be given by the data controller a description of:
- the personal information held about that individual;
  - the purposes for which they are being or are to be processed; and
  - the recipients or classes of recipients to whom the personal information is being or may be disclosed
- (c) to have communicated to him or her in an intelligible form:
- the personal information held about that individual; and
  - any information available to the data controller as to the source of that personal information, and
- (d) to be informed by the data controller of the logic involved in decision-taking where there is processing by automatic means of personal information about that individual for the purpose of evaluating matters relating to him or her (such as, for example, his or her performance at work, his or her creditworthiness, his or her reliability or his or her conduct) which constituted or is likely to constitute the sole basis for any decision significantly affecting the individual
12. Section 9A of the DPA 1998 provides limits on the rights of access to manual personal data held by public authorities other than information which is "recorded as part of, or with the intention that it should form part of, any set of information relating to individuals to the extent that the set is structured by reference to individuals or by reference to criteria relating to individuals." The limits mean that if the individual concerned wants access to this kind of manual personal information, he or she must provide a description of the personal data. Also the public authority does not have to comply if it estimates (in accordance with regulations under the FoIA) that the cost of complying would exceed an amount prescribed by statutory instrument from time to time – the current statutory limit is £450 for public authorities which are not government departments or certain other central government bodies. However, the requirement in paragraph 11(a) above will have to be complied with unless it is estimated that compliance with that alone will exceed the £450 limit.
13. By virtue of orders under Section 30 of the DPA 1998 the individual's access to some health, education and social work personal information may be restricted or denied. (See the three "Subject Access Modification" Orders described in part 3 of Appendix 5 to this Protocol.)
14. The DPA 1998 requires all organisations which process personal information to make a formal notification to the Information Commissioner. It is particularly important when engaging in information sharing that the purposes for which the personal information is to be used are

included in the notification - if the notification is incomplete in any way, appropriate amendments must be submitted before processing can start.

### **The Common Law Duty of Confidentiality**

15. The NHS Code of Practice on Confidentiality provides helpful guidance on this aspect.
16. All Personnel working in both the public and private sectors should understand that they are subject to the common law duty of confidentiality, and must abide by this. The duty of confidentiality applies to information about an identifiable individual and not to aggregated data derived from such personal information or to personal information that has otherwise been effectively anonymised — i.e. it is not possible for anyone to link the information to a specific individual.
17. The duty of confidentiality means that confidential information should only be used for purposes that the subject has been informed about and has consented to unless:
  - (a) there is a statutory requirement to use information that has been provided in confidence; or
  - (b) if the holder of the confidential information can justify disclosure as being in the public interest (e.g. to protect others from harm).
18. Whilst it is not entirely clear under law whether a common law duty of confidentiality extends to deceased persons, the Department of Health and professional bodies responsible for setting ethical standards for health professionals accept that it does extend to deceased persons.
19. Unless there is a sufficiently robust public interest justification for using confidential information that has been provided in confidence then the consent of the individual concerned should be obtained (deceased individuals may have provided their consent before death). For living individuals, Schedules 2 and 3 of the DPA 1998 apply in addition whether or not the personal information was provided in confidence.
20. 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 that decisions about treatment, 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.

### **The Caldicott Principles**

21. Both Social Services departments and NHS organisations are committed to the Caldicott Principles when considering whether confidential information should be shared. These are:
  - (a) justify the purpose(s) for using confidential information;
  - (b) only use when absolutely necessary;
  - (c) use the minimum that is required;
  - (d) access should be on a strict “need to know” basis;
  - (e) everyone must understand his or her responsibilities;
  - (f) understand and comply with the law

### **The Human Rights Act 1998 (“HRA”)**

22. Article 8.1 in Schedule 1 of the HRA establishes a right to ‘respect for private and family life’. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health and social care records. This is however a qualified right, so there are specified grounds upon which it may be legitimate for authorities to override or limit those rights. Current understanding is that compliance with the DPA 1998 and the common law of confidentiality should satisfy HRA requirements.
23. Legislation generally must also be compatible with HRA, so any proposal for setting aside obligations of confidentiality through legislation must:
  - (a) pursue a legitimate aim;
  - (b) be considered necessary in a democratic society; and
  - (c) be proportionate to the need,and more generally there is a requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need.
24. In the event of a claim arising from the HRA that an organisation has acted in a way which is incompatible with the HRA rights, a key factor will be whether the organisation can show, in relation to its decision to take a particular course of action:
  - (a) that it has taken these rights into account;
  - (b) that it considered whether any breach may 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.
25. 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 HRA.

### **The Access To Health Records Act 1990 (“AHRA”)**

26. The DPA 1998 supersedes the AHRA apart from the sections dealing with access to information about the deceased. The AHRA provides rights of access to health records of deceased individuals for their personal representatives and others having a claim on the deceased’s estate. In other circumstances, disclosure of health records relating to the deceased should be carried out in such a way as to comply with the common law duty of confidentiality.

### **Freedom Of Information Act 2000 (“FoIA”)**

27. For public bodies, the FoIA will extend access rights to information to allow access to all the types of information held, whether personal or non-personal. However, the public authority will not be required to release information to which any of the exemptions in the FoIA applies.

Anyone will be able to make a request for information, although the request must be in a permanent form. The FOIA gives applicants two related rights:

- (a) the right to be told whether the information exists;
- (b) the right to receive the information (and where possible, in the manner requested, i.e. as a copy or summary, or the applicant may ask to inspect a record).

28. All the Parties to this Protocol are subject to the provisions of the as well as the DPA 1998. In terms of this Protocol, how FOIA deals with personal data and interacts with the DPA 1998 is important. In general terms, where the information requested under the FOIA contains personal data relating to the applicant, the request is to be treated as a request under the DPA 1998.

### **The Crime and Disorder Act 1998 (“CDA”)**

29. The CDA introduces measures to reduce crime and disorder, including the introduction of local crime prevention partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area. Section 115 of the CDA 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 CDA.
30. Section 115 does not place information holders under a duty to disclose, nor does it give those making requests any power to demand disclosure. All disclosures must comply with the data protection principles (and so the discloser would want to be satisfied that the “crime and taxation” exemption in Section 29 of the DPA 1998 applies and the conditions in Schedules 2 and 3 of the DPA 1998 were satisfied) and other legal requirements, such as the common law duty of confidentiality.

### **The Criminal Procedures And Investigations Act 1996 (“CPIA”)**

31. The CPIA means that information supplied to the police may be disclosed onward by the police to a defendant. The CPIA requires the police to record in a durable form any information that is relevant to an investigation. The information must be disclosed to the Crown Prosecution Service (“CPS”), who must in turn disclose it to the defence at the relevant time if it might undermine the prosecution case. In cases where the information is deemed to be of a sensitive nature, then the CPS can apply to a judge or magistrate for a ruling as to whether it should be disclosed.

### **Regulation Of Investigatory Powers Act 2000**

32. This Act is for the purpose of ensuring that investigatory powers are used in accordance with human rights.

### **Health and Social Care Act 2001**

33. Section 60 of the HSCA gives the Secretary of State the power to make regulations relating to the processing of prescribed patient information for medical purposes in the interests of patients or the wider public good (e.g. disclosing patient identifiable information to specified bodies, such as cancer registries).
34. The proposed use of patient identifiable information for which regulations under Section 60 are made must be acceptable under the HSCA. Acceptable purposes are preventative medicine, medical diagnosis, medical research, provision of care and treatment, management

of health and social care services and informing individuals about their physical or mental health or condition, the diagnosis of their condition or their care or treatment but the primary purpose of the processing cannot be to determine the care and treatment of specific patients.

35. Section 60 does not change the DPA 1998 requirements but where regulations apply it does set aside the legal duty of confidentiality and replace it with a range of safeguards intended to ensure that the use of a patient's information has no detrimental effect on that patient. The existing regulations under Section 60 are in the Health Service (Control of Patient Information) Regulations 2002.

**APPENDIX 3**

**DISCLOSURE OF INFORMATION BETWEEN PERSONNEL IN DIFFERENT ORGANISATIONS.**

**FORMS FOR USE IN COMPLYING WITH THIS PROTOCOL**

	page
<b>FORM A: Disclosure Request Form</b>	<b>39</b>
<b>FORM B: Information Sharing Record Form</b>	<b>41</b>
<b>FORM C: Disclosure In Circumstances Of Risk Form</b>	<b>44</b>
<b>FORM D: Service User Consent to Share Specific Information</b>	<b>47</b>
<b>FLOW DIAGRAM - For use of Forms.</b>	<b>49</b>

## Disclosure Request Form (FORM A)

**Guidance Notes:**

This form must be completed when requesting personal information from an outside organisation. All parts must be completed, dated and signed by the member of staff requesting the disclosure.

This document is to be filed in the service user's records.

Remember that disclosure of "sensitive personal data" will require the service user's explicit consent unless a statutory exception exists.

<u>Service user personal information</u>			
<b>Name:</b>			
<b>Address:</b>			
<b>Telephone:</b>			
<b>DOB:</b>			
<b>NHS Number:</b>		<b>Gender:</b>	
<u>Requesting Party's Information</u>			
<b>Name:</b>			
<b>Organisation:</b>			
<b>Contact Information:</b>			
<b>Information Requested:</b>			
<b>Purpose:</b>			

East London Inter Organisational General Protocol For Sharing Information

<p><b>Signed:</b></p>	<p>The Requesting Party named above hereby:</p> <ol style="list-style-type: none"> <li>1. agrees that (except as otherwise permitted by law) it shall only use the personal information requested above for the specific purpose for which it was intended;</li> <li>2. confirms that it understands that this personal information has been provided in confidence by the individual to whom the personal information pertains; and</li> <li>3. agrees that it will not be further disclosed, or shared with another organisation unless prior consent has been sought and agreed or it is otherwise permitted by law.</li> </ol> <p>..... <b>Date:</b></p>
<p><b>Name and position (Block Capitals)</b></p>	
<p><b>Authorisation Signature:</b></p>	<p style="text-align: right;"><b>Date:</b></p>
<p><b>Name and position (Block Capitals)</b></p>	

## Information Sharing Record Form (FORM B)

**Guidance notes:**

**This form must be completed when sharing personal information with another organisation. It should be completed in response to a Disclosure Request Form, or indeed any request for personal information that is non-urgent in nature. All parts must be filled in, dated, and signed by the member of staff responding to the request for disclosure.**

**Personnel should note that consent is not required in all circumstances for sharing information, e.g. in life or death, emergency and high-risk circumstances. Details of circumstances where consent is not required can be obtained from your organisation’s data protection officer or Caldicott Guardian or equivalent office.**

**This document is to be filed in the service user’s records.**

**Remember that disclosure of “sensitive personal data” will require the service user’s explicit consent unless a statutory exception exists.**

<u>Service user Information</u>			
Name:			
Address:			
Telephone:			
DOB:			
NHS Number:		Gender:	
<u>Requesting Organisation</u>			
Name:			
Organisation:			
Designation:			
Contact Information:			

<b>Information Requested:</b>	
<b>Purpose:</b>	
<b><u>Disclosing Organisation</u></b>	
<b>Name:</b>	
<b>Organisation:</b>	
<b>Contact Information:</b>	
<b>Information Tendered:</b>	
<b>Limitations on Disclosure:</b>	
<b>Is any of the information requested “sensitive personal data”?</b>	
<b>Has the Service User consented to this disclosure?</b>	
<b>In the case of “sensitive personal data”, was the consent explicit?</b>	
<b>If the answer is “no” to either of</b>	

East London Inter Organisational General Protocol For Sharing Information

<b>the previous questions, then justify disclosure.</b>	
<b>Signed:</b>	<b>Date</b>
<b>Name and position (Block Capitals)</b>	
<b>Authorisation Signature:</b>	<b>Date:</b>
<b>Name and position (Block Capitals)</b>	

## Disclosure In Circumstances Of Risk Form (FORM C)

**Guidance Notes:**

This form is for completion where personal information is to be shared in circumstances of risk and without the consent of the service user to whom the personal information relates.

Not seeking such consent and/or overriding the expressed wishes of the service user and/or the person entitled to give consent on such service user's behalf can only happen where there is a clear statutory or other legal right or duty to do so. The details of such decisions should be recorded via this 'risk assessment' form.

*All parts of this document must be completed where appropriate, dated and signed by those indicated on the form.*

*This document is to be filed in the service user's records.*

<u>Service user Information</u>			
<b>Name:</b>			
<b>Address:</b>			
<b>DOB:</b>			
<b>NHS Number:</b>		<b>Gender:</b>	
<u>Organisation That Originally Collected The Personal information</u>			
<b>Organisation:</b>			
<b>Care Coordinator or Senior Clinician:</b>			
<b>Designation:</b>			
<b>Contact Information:</b>			

<b>Has a formal request for personal information been received?</b>		<b>Yes</b>	<b>No</b>
<b><u>Organisation to which the Personal Information is proposed to be Disclosed</u></b>			
<b>Name:</b>			
<b>Organisation:</b>			
<b>Designation:</b>			
<b>Contact Information:</b>			
<b>Information Requested:</b>			
<b>Purpose:</b>			
<b>Has the service user given consent to share?</b>		<b>Yes</b>	<b>No</b>
<b>If the answer to this question is “No” you need to complete the Risk Assessment section that follows.</b>			

**Risk Assessment**

<b>Professional risk assessment will often be the only justifiable reason in law, for breaching the confidentiality and security of personal information, without the informed consent of the individual concerned.</b>		
<b>Has, or is a formal risk assessment of the service user’s circumstances planned, or been conducted?</b>	<b>Yes</b>	<b>No</b>
<b>Outcome of Risk Assessment:</b>		

East London Inter Organisational General Protocol For Sharing Information

<b>Information to be shared:</b>			
<b>With whom &amp; for what purpose:</b>			
<b>Was this personal information shared with the Requesting Organisation?</b>	<b>Yes</b>	<b>No</b>	

## Service User Consent to Share Specific Information (FORM D)

Guidance Notes:

This form should be completed in situations where it appears consent to share personal information with another organisation is required from the service user. The service user has the right to refuse to give such consent, as does their legally designated representative. The individual can also apply limitations upon the disclosure of personal information, and with whom. They also have the right to apply a time scale to the sharing this personal information.

All parts of this document must be completed where appropriate, dated and signed by those indicated on the form.

This document is to be filed in the service user's records.

**To achieve 'informed' consent, either the individual and/or the legally designated representative must be fully briefed of the implications of such consent.**

<b>Who has been briefed?</b>	<b>Service User</b>	<b>Legally Designated Representative</b>
<b>Limitations on Disclosure:</b>		
<b>Timescales (if indicated):</b>		
<b>Organisations with whom and amongst whom personal information will be shared &amp; why:</b>		
<p><b>I agree to the above personal information being shared with the organisations noted above, for the purposes stated.</b></p> <p><b>Signed:</b> _____ <b>Date:</b> _____</p>		
<p><b>(To be completed where appropriate)</b>  <b>I am the service user's legal guardian, and I agree with the above personal information being shared with the organisations noted above, for the purposes stated.</b></p> <p><b>Signed:</b> _____ <b>Date:</b> _____</p>		
<b>Staff signature:</b>	<b>Date:</b> _____	

East London Inter Organisational General Protocol For Sharing Information

<b>Designation:</b>	
<b>Authorisation Signature:</b>	<b>Date:</b>
<b>Designation:</b>	

A copy of this document must be given to the service user and/or their designated legally authorised representative. Where a formal risk assessment would indicate actual/or potential danger to others if given to the individual, then a copy of this document can be withheld from the service user but such a decision must be recorded on the form.

This document must be placed prominently on the service user's record. It is the duty and responsibility of the member of staff completing this document that it is made available to all those that Need to Know, within any of the limitations noted above.



## **APPENDIX 4**

### **PRO-FORMA FOR SUBJECT SPECIFIC INFORMATION SHARING AGREEMENT**

In drawing up individual protocols for sharing information, partners will agree the “rules” for access by going through the following steps for each service area:

- Identify the staff roles where there is a legitimate interest in sharing information
- Define the specific elements of information required for each role
- Identify the reasons the information is required for each role
- Create a matrix showing the elements of information, who “needs to know” and therefore has access to them and the reasons why

Each SSISA shall require the parties to it to implement and maintain procedures for recording, and alerting its Personnel to, any request or requirement imposed by an individual that personal information about him or her shall not be shared with any particular person or class or classes of person.

It is suggested that each SSISA should also include a summary of the information about “consent”, “Need to Know” and the various “exemptions” as well as flow charts.

**Document Control**

Status of document	DRAFT FOR CONSULTATION/ APPROVED
Version	XXXXXXXXXXXXXXXX
Author(s)	XXXXXXXXXXXXXXXX
Date issued	XXXXXXXXXXXXXXXX
Date it was or will be effective from	XXXXXXXXXXXXXXXX
Date of the next scheduled review	XXXX months from date issued

By entering into this SSISA you are affirming that you are aware of your responsibilities for this data flow and that you understand and are complying with the law as per Caldicott principles 5 & 6.

Principle 5: Everyone should be aware of their responsibilities.

Principle 6: Understand and comply with the law.

**KEY**

**1. TEXT IN BLUE – YOU NEED TO FILL IN INFORMATION.** Then delete my blue bits.

**2. TEXT IN RED – ADVICE/GUIDANCE.** - This is guidance to help you complete the SSISA, it is **not** part of the SSISA, when you have finished writing the SSISA please delete all the text in red.

**3. TEXT HIGHLIGHTED IN YELLOW** REFERS YOU TO AN **ANNEX** WHICH YOU HAVE TO COMPLETE.

# Subject Specific Information Sharing Agreement “SSISA”

## Between

XX

[NAME THE AGENCIES INVOLVED]

e.g. Barts and the London NHS Trust, London Borough of Hackney

## agencies in

XXXXXXX

e.g. East London, London, UK, etc.,

## for the purpose of

XX

e.g. Providing patient details to other NHS Trusts/ local government/voluntary agencies involved in ongoing service user/patient care.

e.g. Clinical audit.

e.g. SAP – single assessment process.

## JUSTIFICATION OF PURPOSE

XX

A JUSTIFICATION FOR THE PURPOSE SHOULD ALSO BE INCLUDED. i.e. WHY THERE IS A NEED FOR THIS INFORMATION TO BE SHARED.

AS PER CALDICOTT PRINCIPLE 1 - “Justify the purpose[s] for using confidential information.”

e.g. PURPOSE = SAP

The Department of Health requires organisations involved in the ongoing treatment and care of older patients/service users who are subject to the Single Assessment Process to share relevant assessment information with each other. The personal information contained in the Current Summary Record will be shared with staff from NHS Trusts, social care and other organisations involved in an individual patient’s/service user’s care network to enable the efficient delivery of ongoing treatment and care to the individual patient/service user. The information will also be used to assist with organisations’ clinical audit and performance management responsibilities.

## 1. PARTIES

The Parties to this SSISA (the “Parties”) are:

e.g.

- East London & The City Mental Health NHS Trust,
- Barts and The London Hospitals NHS Trust,

whose addresses are as set out in **Annex A** below.

[NB Include above only those organisations that are to be party to this SSISA - Any parties to this SSISA who are not already signatories of the Protocol defined in paragraph 1 below should note that by becoming signatories of an SSISA using this form, by virtue of paragraph 3.1.2 they will be required to comply with that Protocol in so far as it is relevant to the information sharing to which this SSISA relates.]

## 1. DEFINITIONS

In this SSISA, the following terms have the following meanings:

“Committee”	has the meaning in the Protocol
“Care Service”	has the meaning in paragraph 2 below
“DPA 1998”	the Data Protection Act 1998
“Explicit Consent”	has the meaning described in paragraph 10.3 of Appendix 1 to the Protocol
“Need to Know”	has the meaning described in paragraph 5 of Appendix 1
“other SSISA”	any Subject Specific Information Sharing Agreement to which the Protocol relates and to which some or all of the Parties are party, other than this SSISA
“personal information”	“personal data” as defined in the DPA 1998
“Personnel”	the Parties’ employees, officers, elected members, directors, voluntary staff, consultants and other contractors and their sub-contractors (whether or not subject to legally binding contracts) and such contractors’ and their sub-contractors’ Personnel
“the Protocol”	the “East London Health & Social Care Inter Organisation General Protocol For Sharing Information” established by a memorandum of agreement to which the Parties are signatories
“receiving Party”	has the meaning in paragraph 4.3.1 below
“sensitive personal data”	has the meaning in the Protocol
“service users”	the individuals who are recipients of the Parties’ health and care services and because service users and other individuals about whom personal information is held will be “data subjects” within the meaning of the DPA 1998, in this SSISA where the context so allows “service users” will include any such data subjects
“SSISA”	Subject Specific Information Sharing Agreement

## 2. THE SUBJECT OF THIS SSISA

2.1 The care service to which this SSISA relates is **NAME THE SERVICE**

[Describe the care process which this SSISA addresses e.g. Cardiac Rehabilitation, Children’s Services, SAP.]

- 2.2 The purpose of this SSISA is to identify:
- 2.2.1. the procedures for secure and confidential sharing of information between the Parties in the course of the delivery of the Care Service;
  - 2.2.2. the specific purposes for which the Parties have agreed to share personal information in connection with delivery of the Care Service;
  - 2.2.3. the responsibilities assigned to the Parties in relation to the collection of personal information;
  - 2.2.4. the responsibilities of each Party to implement procedures to seek to obtain the consent of service users for the sharing of their personal information; and
  - 2.2.5. how this SSISA will be implemented, monitored and reviewed.
- 2.3. Each Party warrants to the others that:
- 2.3.1. it has full power and authority to enter into and perform this SSISA and when signed on such Party's behalf this SSISA will constitute binding obligations on such Party in accordance with this SSISA's terms; and
  - 2.3.2. its signatory identified below in annex A is duly authorised to sign this SSISA on behalf of such Party.
- 2.4. Each Party undertakes to the others that it and its Personnel will comply with this SSISA and the law relevant to the information sharing to which this SSISA relates.

### 3. SCOPE

#### 3.1. Application and Indemnities

3.1.1. The Parties to this SSISA who are also parties to the Protocol agree that as between themselves:

- 3.1.1.1. this SSISA is subject and subservient to the Protocol; and
- 3.1.1.2. the provisions of the Protocol apply to and are deemed included in this SSISA.

3.1.2. If any Party to this SSISA is not already a party to the Protocol, or subsequently ceases (whether by temporary or permanent suspension or otherwise) to be a party to the Protocol, by entering into this SSISA such Party undertakes in favour of all parties to the Protocol to comply (or, as the case may be, continue to comply) with the terms of the Protocol insofar as it is relevant to the information sharing to which this SSISA relates.

3.1.3. The fact that a Party has ceased (whether by temporary or permanent suspension or otherwise) to be a party to the Protocol **SHALL NOT OF ITSELF** be a reason for a Party not to share personal information with any such suspended Party, bearing in mind the underlying importance of the health and well-being of service users and others.

3.1.4. Clauses 3.4.1 to 3.4.7 (headed "Indemnity Agreement") of the Protocol shall be deemed to be repeated in this SSISA but as though references in those clauses to the Protocol were deemed to be references to this SSISA and references to "a Party" or "Parties" were to a Party or Parties to this SSISA.

#### 3.2. Relationship to other SSISAs between the Parties:

If this SSISA applies to subject matter to which any other SSISA applies, nothing in this SSISA shall prejudice such other SSISA, provided that if there shall be any conflict between this SSISA and such other SSISA it shall be resolved by agreement between the Parties and the parties to such other SSISA or in the absence of such agreement then at the request of any party to this SSISA or such other SSISA by decision of the Committee.

### 3.3 Care Service roles of the Parties

It is anticipated that the following Parties will perform the following roles in respect of the Care Service, as detailed in **Annex B**.

[Complete the table in Annex B with an entry for each Party]

### 3.4 Management of service user risk

In addition to their Care Service roles identified above, the Parties recognise that they need to share information about individuals who they suspect have been subject to, or may be at risk of, abuse and individuals who may be responsible for perpetrating abuse. They will share personal information known to them about such individuals as openly as possible with other Parties' Personnel who Need to Know, albeit in a manner which is compliant with their statutory responsibilities, the Protocol and this SSISA. Examples of circumstances where sharing of personal information may be required because a service user or some other person is at risk include:

- (a) to raise grounds for concern about a person believed to be at risk of abuse;
- (b) to notify agencies who have a responsibility to take action in respect of a person who may be at risk of abuse;
- (c) to notify the Parties of staff who are thought to pose a risk in relation to the nature of their employment;
- (d) to notify Parties of a risk posed by a service user;
- (e) to make a referral to agencies for the purposes of requesting or amending services both for persons at risk of abuse and for those suspected of perpetrating abuse; or
- (f) to deal effectively with complaints, grievances and professional and administrative malpractice.

## 4. PROCEDURES

### 4.1. Internal compliance with this SSISA

Each Party shall instruct its Caldicott Guardian, data protection officer or equivalent for the time being to oversee compliance with this SSISA within such Party's organisation.

See **Annex C** below for a list of named individuals in each party responsible for compliance and information sharing issues to which this SSISA relates.

[Complete the table in Annex C with an entry for each Party]

### 4.2. The Collection Of Personal Information

4.2.1. Personal information relevant to the Care Service to which this SSISA relates will be collected in accordance with the following processes:

- (a) a collection process set out in **Annex D** below.

[annex D will hold all the details of how the information will be collected and a description of the information to be collected, you need to fill this in]

4.2.2. Each Party agrees that:

- (a) it is responsible for maintaining the personal information that it has collected on its own account, or jointly with another Party, in accordance with the DPA 1998;
- (b) it will retain legal responsibility for correcting personal information where it is factually incorrect; and

- (c) it will not amend the record of an opinion or judgement recorded by a health or social care professional, whether accurate or not, because the recorded opinion or judgement is essential for understanding the clinical decisions that were made and to audit the quality of care.

#### 4.3. Dissemination Of Personal Information

4.3.1. Wherever possible, subject to paragraphs 4.4 and 4.5 below and the requirements of the Protocol and applicable law and guidance, personal information collected by one Party that is requested by another Party (or is proposed to be transferred to another Party without a request) for the purposes of the Care Service, will be transferred to the proposed recipient Party ("**the receiving Party**") as:

- (a) part of any referral correspondence; and/or
- (b) part of an 'at risk' alert.

4.3.2. After receipt of the shared personal information the receiving Party will, for the purpose of protecting the service user's welfare, promptly pass to the Party which shared it:

- (a) progress reports on the nature of the care provided by the receiving Party and the outcomes planned; and
- (b) discharge correspondence when the care provision has ceased.

[add anything else appropriate to this particular Care Service]

[paragraph 4.3.2 above only needs to be included where it is relevant to the kinds of service to which the SSISA relates]

#### 4.4. Sharing of Personal Information

4.4.1. Personal information may be disclosed to a receiving Party only if the personal information is necessary to perform a function or responsibility identified for such receiving Party to perform in the table in paragraph 3.3 above and (if there has been a request) the request for the information has been made in accordance with the procedures in appendix 1 of the Protocol.

[that's the guidance section, "information sharing principles". you can copy this section of the protocol into the SSISA as an annex if you wish].

**UNLESS:**

- (a) the service user or some other person to whom such personal information relates has refused consent for the sharing of such personal information; or
- (b) the personal information is sensitive personal data as defined by the DPA 1998 and paragraph 4.5 below does not permit its disclosure.

4.4.2. The persons holding the job titles listed in the table in **Annex E**, and only those persons, will be permitted access to personal information shared under this SSISA which is not sensitive personal data.

Alterations from time to time to the above list shall be notified by the Parties to each other in accordance with paragraph 9.4 below.

#### 4.5. Sharing of Sensitive Personal Data

4.5.1. Sensitive personal data may be disclosed to a receiving Party **ONLY IF:**

- (a) the sensitive personal data is necessary to perform a function or responsibility identified for such receiving Party to perform in the table in paragraph 3.3 above and (if there has been a request) the request for the information has been made in accordance with the procedures in appendix 1 of the Protocol.

[that's the guidance section, "information sharing principles". you can copy this section of the protocol into the SSISA as an annex if you wish].

AND EITHER

- (b) the service user or other person to whom such sensitive personal data relates has given his or her Explicit Consent for the sharing of such sensitive personal data;

OR

- (c) some other lawful ground for sharing the sensitive personal data without Explicit Consent exists as described in the Protocol appendix 1 section 13.

4.5.2. Each Party's Caldicott Guardian, data protection officer or equivalent shall:

- (a) notify the other Parties' Caldicott Guardians, data protection officers or equivalent of the roles of persons in such Party who will be permitted access to sensitive personal data held by such Party and any changes to such list from time to time; and
- (b) maintain a list of the roles of persons in each of the Parties who will be permitted access to sensitive personal data held by the Parties,

and only those persons whose roles are identified on the list kept by the Parties' Caldicott Guardians, data protection officers or equivalent shall have access to sensitive personal data. All persons whose roles are identified on such list will be provided with a copy of the list to enable them to be fully aware of the identity of persons with whom they are authorised to share information. The list may be qualified, and access to sensitive information further protected, by limiting access to information by some persons on the list in relation to specifically named service users.

4.5.3. The persons holding the job titles listed in the table in **Annex E**, and only those persons, will be permitted access to personal sensitive information shared under this SSISA. Alterations from time to time to such list shall be notified by the Parties to each other in accordance with paragraph 9.4 below.

#### 4.6. Audit Trail Procedure

The Parties shall abide by the audit trail procedure as set out in **Annex F**.

### 5. SERVICE PLANNING, COMMISSIONING, STATUTORY RETURNS AND REVIEW

#### 5.1 Procedure for sharing information for service planning, commissioning, statutory returns and review

5.1.1. The Parties recognise that service planning, commissioning, statutory returns and review requires sharing of information about the incidence and nature of the contribution that they make to service users' care.

5.1.2. **[DELETE OR ADD PROCEDURE BELOW AS APPROPRIATE]**

**[either]**

The Parties will anonymise information before they make it available for service planning, commissioning, statutory returns and review purposes.

**[Or]**

Sharing information for service planning, commissioning, statutory returns and review purposes will strictly follow the procedure below, which has been approved by the Parties' respective Caldicott Guardians, data protection officers or equivalent. This procedure is detailed in Annex H.

**[In Annex I describe the procedure for information sharing for service planning and review if you will not be anonymising the information]**

### 6. SPECIFIC ARRANGEMENTS

See **Annex G** for procedures for transfer of data, updating of data and transfer of data in emergencies or transfer to non signed up organisations.

## 7. AGREED GUIDANCE FOR STAFF

The information contained in **Annex H** is agreed between the Parties as practice that must be complied with to help ensure consistency in the processes adopted in sharing personal information.

[This paragraph 7 is optional. Those making use of this paragraph 7 should take care not to conflict with any commitments made in the Protocol, which overrides this SSISA, or with the general law. Further, any Parties intending to produce and rely upon such an Annex are advised to obtain legal advice on it.]

## 8. NO THIRD PARTY RIGHTS

Save as provided in paragraph 3.1.2 above, each Party agrees that no term of this SSISA is enforceable under the Contracts (Rights of Third Parties) Act 1999 by a person who is not a Party to this SSISA.

## 9. GENERAL

9.1 In this SSISA:

- (a) words importing one gender shall (where appropriate) include any other gender and words importing the singular shall (where appropriate) include the plural and vice versa;
- (b) references to statutory provisions shall be construed as references to those provisions as amended or re-enacted or as their application is modified by other provisions from time to time (whether before or after the date of this SSISA) and shall include references to any provisions of which they are re-enactments (whether with or without modification) and shall also include statutory instruments or orders from time to time (whether before or after the date of this SSISA) made pursuant to them;
- (c) unless the context otherwise requires, references to paragraphs and to appendices are to paragraphs of and appendices to this SSISA

9.2 No variation, waiver or modification of any of the terms of this SSISA shall be valid unless in writing and signed by or on behalf of the authorised representatives of the Parties.

9.3 Nothing in this SSISA shall constitute or be deemed to constitute a legal partnership between any of the Parties or any Party the agent of any other Party and none of them shall have any authority to bind the others in any way by virtue of this SSISA, save as otherwise expressly provided in this SSISA.

9.4 All notices to be given under this SSISA will be in writing and will be sent to the address and contact name for the receiving Party shown in Annex A below or any other address the relevant Party may designate by notice given in accordance with this paragraph 9.4 to all other Parties. Notices may be delivered personally, by first class pre-paid letter or by fax. Notices will be deemed to have been received:

- (a) by hand delivery - at the time of delivery
- (b) by first class post - 48 hours after the date of posting
- (c) by fax – immediately on transmission provided a confirmatory copy is sent by first class pre-paid post or delivered by hand by the end of the next business day

## ANNEX A

### PARTIES TO THE AGREEMENT - ADDRESSES, CONTACTS & SIGNATURES

Fill in the name[s] of the individual[s] with the authority to sign this SSISA for your organisation[s]. Usually this will be a Caldicott, senior board member, an information governance manger, department head etc. This will be the person accountable for this SSISA within your organisation.

<b>Organisation</b>	e.g. John Smith NHS Trust
<b>Address</b>	333 high road
<b>Contact Details</b>	phone number, email address
<b>Signature</b>	Signature of person with full power and authority to enter into and perform this SSISA
<b>Name:</b>	name of person with full power and authority to enter into and perform this SSISA
<b>Designation:</b>	e.g. Caldicott Guardian
<b>Date:</b>	xx.xx.xxxx

<b>Organisation</b>	
<b>Address</b>	
<b>Contact Details</b>	
<b>Signature</b>	
<b>Name:</b>	
<b>Designation:</b>	
<b>Date:</b>	

[add as many people/tables as necessary]

## ANNEX B

### CARE SERVICE ROLES OF THE PARTIES

The following Parties/departments/agencies will perform the following roles in respect of the Care Service.

PARTY	CARE PROCESS ROLE
Name of the organisation or the department etc., who will be involved with this SSISA	i.e. what the organisation will do in this SSISA, a brief description of the aspect of the care process they will be providing.
e.g. Barts and the London NHS Trust	e.g. provision of hospital - based assessment services
e.g. ELC Mental Health Trust	e.g. provision of hospital-based mental health services
e.g. The Smith General Practice	e.g. Provision of community-based medical services
e.g. Hackney Social Services	e.g. provision of child care services





**ANNEX E**

**STAFF ROLES PERMITTED TO ACCESS THE INFORMATION IN THIS SSISA**

When completing this section bear in mind Caldicott Principle 4 – ‘Access should be on a strict need-to-know basis.’

Format the tables as you need, if you will only be sharing personal sensitive information then delete the other table or vice versa.

**1. DETAILS OF STAFF PERMITTED TO ACCESS PERSONAL INFORMATION RELEVANT TO THIS SSISA.**

['job title' could be a named contact if numbers small enough and you're willing to update. If you're only using 'job title' then, if possible use a department contact number/email. If this is not possible, delete the 'contact number/email column']

<u>NAME OF PARTY</u>	<u>JOB TITLE OF STAFF</u>	<u>CONTACT NUMBER/EMAIL</u>
ORG/AGENCY/DEPT NAME	JOB TITLE[S]	PHONE NUMBER/EMAIL

**2. DETAILS OF STAFF PERMITTED TO ACCESS SENSITIVE PERSONAL INFORMATION RELEVANT TO THIS SSISA.**

['job title' could be a named contact if numbers small enough and you're willing to update. If you're only using 'job title' then, if possible, use a department contact number/email. If this is not possible, delete the 'contact number/email column']

<u>NAME OF PARTY</u>	<u>JOB TITLE OF STAFF</u>	<u>CONTACT NUMBER/EMAIL</u>
ORG/AGENCY/DEPT NAME	JOB TITLE[S]	PHONE NUMBER/EMAIL

## ANNEX F

### AUDIT TRAIL DETAILS FOR THIS SSISA

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Insert here, procedures of maintaining an audit trail for the information shared.

i.e. the what, why, where, who, how, when of the information.

This can be as detailed as you like so long as all parties involved understand what they have to do. The examples below just give the bare bones description.

Both sending and receiving parties will keep an audit trail of their actions.

**e.g. The audit trail will include:**

Job role or Name of staff member accessing, collecting or sharing the information.

Organisation name

Action [send/receive]

Date sent or received.

Date of confirmation of receipt.

Identification of information shared.

Confirmation of secure disposal of fax.

How long the information is to be kept.

Secure disposal procedures.

**ANNEX G**

**PROCEDURE FOR TRANSFER OF DATA, UPDATING OF DATA, TRANSFER IN EMERGENCIES AND TRANSFER TO NON SIGNED UP ORGANISATIONS.**

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

- 1. methods for transfer of data, fax, hardcopy, phone etc.,
- 2. how to share with non signed up organisations or in emergencies e.g. use the template forms.[see forms below]
- 3. any specific agreement as to what information is to be subject to updates and whose responsibility it will be to initiate updates.

e.g. The sending organisation will fax the relevant information to the parties concerned from a safe haven fax to a safe haven fax in the receiving organisation. The sending organisation will keep the master on record as well as a fax log of the information transfers.

Recipient parties will confirm receipt of fax by phone. Recipient parties will extract the relevant patient information and shred their copy of the fax in a secure manner.

Both sending and receiving parties will keep an audit trail of their actions.

[the section below has the info sharing forms and the flow diagram to help in using them. You may use these forms or not use them, subject to your SSISA needs]

**Sharing Information with Organisations not signed up to this SSISA**

If information other than that described above needs to be shared, or information needs to be shared outside the scope of this SSISA the following forms shall be used for each transfer of information:

- Complete form A below when requesting information.
  - Complete form B below when sending information
  - Complete from C below when sharing in an emergency or in circumstances of risk
  - Complete form D below to obtain service consent for sharing information.
- [Refer to flow chart below for guidance]

## Disclosure Request Form (FORM A)

**Guidance Notes:**

This form must be completed when requesting personal information from an outside organisation. All parts must be completed, dated and signed by the member of staff requesting the disclosure.

This document is to be filed in the service user's records.

Remember that disclosure of "sensitive personal data" will require the service user's explicit consent unless a statutory exception exists.

<u>Service user personal information</u>			
<b>Name:</b>			
<b>Address:</b>			
<b>Telephone:</b>			
<b>DOB:</b>			
<b>NHS Number:</b>		<b>Gender:</b>	
<u>Requesting Party's Information</u>			
<b>Name:</b>			
<b>Organisation:</b>			
<b>Contact Information:</b>			
<b>Information Requested:</b>			
<b>Purpose:</b>			

East London Inter Organisational General Protocol For Sharing Information

<p><b>Signed:</b></p>	<p>The Requesting Party named above hereby:</p> <ol style="list-style-type: none"> <li>1. agrees that (except as otherwise permitted by law) it shall only use the personal information requested above for the specific purpose for which it was intended;</li> <li>2. confirms that it understands that this personal information has been provided in confidence by the individual to whom the personal information pertains; and</li> <li>3. agrees that it will not be further disclosed, or shared with another organisation unless prior consent has been sought and agreed or it is otherwise permitted by law.</li> </ol> <p>..... <b>Date:</b></p>
<p><b>Name and position (Block Capitals)</b></p>	
<p><b>Authorisation Signature:</b></p>	<p style="text-align: right;"><b>Date:</b></p>
<p><b>Name and position (Block Capitals)</b></p>	

## Information Sharing Record Form (FORM B)

<p><b>Guidance notes:</b></p> <p>This form must be completed when sharing personal information with another organisation. It should be completed in response to a Disclosure Request Form, or indeed any request for personal information that is non-urgent in nature. All parts must be filled in, dated, and signed by the member of staff responding to the request for disclosure.</p> <p>Personnel should note that consent is not required in all circumstances for sharing information, e.g. in life or death, emergency and high-risk circumstances. Details of circumstances where consent is not required can be obtained from your organisation's data protection officer or Caldicott Guardian or equivalent office.</p> <p>This document is to be filed in the service user's records.</p> <p>Remember that disclosure of "sensitive personal data" will require the service user's explicit consent unless a statutory exception exists.</p>
---

<u>Service user Information</u>			
<b>Name:</b>			
<b>Address:</b>			
<b>Telephone:</b>			
<b>DOB:</b>			
<b>NHS Number:</b>		<b>Gender:</b>	
<u>Requesting Organisation</u>			
<b>Name:</b>			
<b>Organisation:</b>			
<b>Designation:</b>			
<b>Contact Information:</b>			
<b>Information Requested:</b>			

<b>Purpose:</b>	
<b><u>Disclosing Organisation</u></b>	
<b>Name:</b>	
<b>Organisation:</b>	
<b>Contact Information:</b>	
<b>Information Tendered:</b>	
<b>Limitations on Disclosure:</b>	
<b>Is any of the information requested “sensitive personal data”?</b>	
<b>Has the Service User consented to this disclosure?</b>	
<b>In the case of “sensitive personal data”, was the consent explicit?</b>	
<b>If the answer is “no” to either of the previous questions, then justify</b>	

East London Inter Organisational General Protocol For Sharing Information

<b>disclosure.</b>	
<b>Signed:</b>	<b>Date</b>
<b>Name and position (Block Capitals)</b>	
<b>Authorisation Signature:</b>	<b>Date:</b>
<b>Name and position (Block Capitals)</b>	

Disclosure In Circumstances Of Risk Form (FORM C)

**Guidance Notes:**

This form is for completion where personal information is to be shared in circumstances of risk and without the consent of the service user to whom the personal information relates.

Not seeking such consent and/or overriding the expressed wishes of the service user and/or the person entitled to give consent on such service user's behalf can only happen where there is a clear statutory or other legal right or duty to do so. The details of such decisions should be recorded via this 'risk assessment' form.

*All parts of this document must be completed where appropriate, dated and signed by those indicated on the form.*

*This document is to be filed in the service user's records.*

<u>Service user Information</u>			
<b>Name:</b>			
<b>Address:</b>			
<b>DOB:</b>			
<b>NHS Number:</b>		<b>Gender:</b>	
<u>Organisation That Originally Collected The Personal information</u>			
<b>Organisation:</b>			
<b>Care Coordinator or Senior Clinician:</b>			
<b>Designation:</b>			
<b>Contact Information:</b>			

<b>Has a formal request for personal information been received?</b>		<b>Yes</b>	<b>No</b>
<b><u>Organisation to which the Personal Information is proposed to be Disclosed</u></b>			
<b>Name:</b>			
<b>Organisation:</b>			
<b>Designation:</b>			
<b>Contact Information:</b>			
<b>Information Requested:</b>			
<b>Purpose:</b>			
<b>Has the service user given consent to share?</b>		<b>Yes</b>	<b>No</b>
<b>If the answer to this question is “No” you need to complete the Risk Assessment section that follows.</b>			

**Risk Assessment**

<b>Professional risk assessment will often be the only justifiable reason in law, for breaching the confidentiality and security of personal information, without the informed consent of the individual concerned.</b>		
<b>Has, or is a formal risk assessment of the service user’s circumstances planned, or been conducted?</b>	<b>Yes</b>	<b>No</b>
<b>Outcome of Risk Assessment:</b>		

East London Inter Organisational General Protocol For Sharing Information

<b>Information to be shared:</b>			
<b>With whom &amp; for what purpose:</b>			
<b>Was this personal information shared with the Requesting Organisation?</b>	<b>Yes</b>	<b>No</b>	

## Service User Consent to Share Specific Information (FORM D)

Guidance Notes:

This form should be completed in situations where it appears consent to share personal information with another organisation is required from the service user. The service user has the right to refuse to give such consent, as does their legally designated representative. The individual can also apply limitations upon the disclosure of personal information, and with whom. They also have the right to apply a time scale to the sharing this personal information.

All parts of this document must be completed where appropriate, dated and signed by those indicated on the form.

This document is to be filed in the service user's records.

**To achieve 'informed' consent, either the individual and/or the legally designated representative must be fully briefed of the implications of such consent.**

<b>Who has been briefed?</b>	<b>Service User</b>	<b>Legally Designated Representative</b>
<b>Limitations on Disclosure:</b>		
<b>Timescales (if indicated):</b>		
<b>Organisations with whom and amongst whom personal information will be shared &amp; why:</b>		
<p>I agree to the above personal information being shared with the organisations noted above, for the purposes stated.</p> <p><b>Signed:</b> _____ <b>Date:</b> _____</p>		
<p><b>(To be completed where appropriate)</b>                  I am the service user's legal guardian, and I agree with the above personal information being shared with the organisations noted above, for the purposes stated.</p> <p><b>Signed:</b> _____ <b>Date:</b> _____</p>		
<b>Staff signature:</b>	<b>Date:</b> _____	
<b>Designation:</b>		

East London Inter Organisational General Protocol For Sharing Information

<b>Authorisation Signature:</b>	<b>Date:</b>
<b>Designation:</b>	

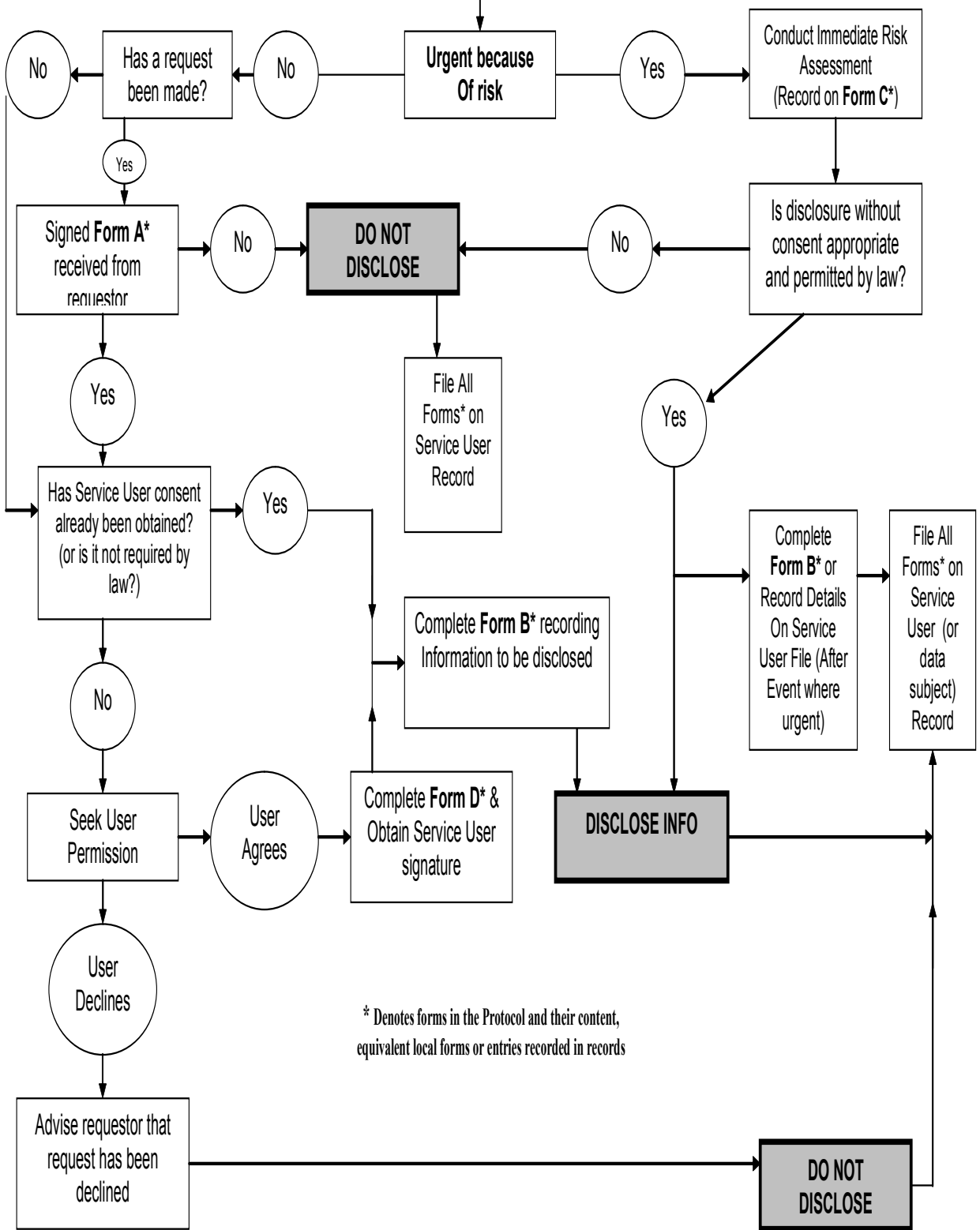
A copy of this document must be given to the service user and/or their designated legally authorised representative. Where a formal risk assessment would indicate actual/or potential danger to others if given to the individual, then a copy of this document can be withheld from the service user but such a decision must be recorded on the form.

This document must be placed prominently on the service user's record. It is the duty and responsibility of the member of staff completing this document that it is made available to all those that Need to Know, within any of the limitations noted above.

**Flow diagram for guidance in use of forms**

**Information Sharing is proposed but is not covered by a SSISA**

**Flowchart - V4**



\* Denotes forms in the Protocol and their content, equivalent local forms or entries recorded in records

## **ANNEX H**

### **AGREED GUIDANCE FOR STAFF [Practice for consistency of Processes]**

[NB The use of this Annex is optional – see paragraph 7 above – and I've stuck a copy of it below.]

**Paragraph 7:**

'This paragraph 7 is optional. Those making use of this paragraph 7 should take care not to conflict with any commitments made in the Protocol, which overrides this SSISA, or with the general law. Further, any Parties intending to produce and rely upon such an Annex are advised to obtain legal advice on it.'

Add any legal or organisational guidance that you feel is appropriate to this particular SSISA  
e.g. Caldicott principles, specific legal guidance such as for STD information, summary of data protection act.,  
general or specific do's and don'ts of information sharing.

## **ANNEX I**

### **DESCRIPTION OF PROCEDURE FOR USING NON ANONYMISED INFORMATION FOR SERVICE PLANNING, COMMISSIONING, STATUTORY RETURNS AND REVIEW**

If you intend to use the information that is being shared according to this SSISA for service planning or review purposes and you do not intend to anonymise it, then describe in this annex the procedure you will use to safeguard the information from being misused. If you anonymise it delete this annex.

When completing this section bear in mind Caldicott Principle 4 – ‘Access should be on a strict need-to-know basis.’

e.g. Written permission is obtained from the treating consultant to send the personal information, the information is encrypted/password protected/pseudonymised and sent from a safe haven fax to a safe haven fax. The receiving party confirms receipt of the information by phone. This is logged by both parties.

e.g. Staff are informed that CRB checks will be made. Staff provide explicit written consent on the CRB form agreeing to transfer of their personal information. The forms are transferred to the CRB in secure opaque envelopes using a specialist secure courier service. Confirmation of receipt is made by phone to a dedicated number and contact name.

## APPENDIX 5

(NOTE: The law in this Appendix is stated as at 31 July 2005)

### Part 1 – DATA PROTECTION ACT 1998 CONDITIONS FOR PROCESSING Non “Sensitive Personal Data”

At least one of the following six conditions must be met in the case of all processing of personal information (except where a relevant exemption applies):-

1. The individual has given his consent to the processing.
2. The processing is **necessary**:
  - (a) for the performance of a contract to which the individual is a party; or
  - (b) for the taking of steps at the request of the individual with a view to entering into a contract.
3. The processing is **necessary** to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is **necessary** in order to protect the vital interests of the individual.

(The Information Commissioner has indicated that reliance on this condition may only be claimed where the processing is necessary for matters of life and death, for example, the disclosure of an individual's medical history to a hospital casualty department treating the individual after a serious road accident.)
5. The processing is **necessary**:
  - (a) for the administration of justice;
  - (b) for the exercise of any functions conferred by or under any enactment;
  - (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or
  - (d) for the exercise of any other functions of a public nature exercised in the public interest.
6. The processing is **necessary** for 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 because of prejudice to the rights and freedoms or legitimate interests of the individual.

**Part 2 – DATA PROTECTION ACT 1998 CONDITIONS FOR PROCESSING  
“Sensitive Personal Data”**

At least one of the following conditions must be satisfied, in addition to at least one of the conditions for processing in Part 1 of this Appendix 5 (which apply to the processing of all personal information), before processing of sensitive personal data can comply with the First Principle of the DPA 1998:-

- 1 The individual has given his **explicit** consent to the processing of the personal information.
- 2 The processing is **necessary** for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services) and is undertaken by:
  - (a) a health professional (as defined in section 69 of the DPA 1998); or
  - (b) a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
- 3 The processing is **necessary** for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(The Secretary of State may specify cases by order where this condition is either excluded altogether or only satisfied upon the compliance with further conditions.)
- 4 The processing is **necessary**:
  - (a) in order to protect the vital interests of the individual or another person, in a case where:
    - (i) consent cannot be given by or on behalf of the individual, or
    - (ii) the data controller cannot reasonably be expected to obtain the consent of the individual, or
  - (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the individual has been unreasonably withheld.
- 5 The processing –
  - (a) is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade union purposes **and** which is not established or conducted for profit;
  - (b) is carried out with appropriate safeguards for the rights and freedoms of individuals;
  - (c) relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes; and
  - (d) does not involve disclosure of the personal information to a third party without the consent of the individual.
- 6 The information contained in the personal information has been made public as a result of steps deliberately taken by the individual.
- 7 The processing:

- (a) is **necessary** for the purpose of, or in connection with, any legal proceedings), (including prospective legal proceeding).
- (b) is **necessary** for the purpose of obtaining legal advice, or
- (c) is otherwise **necessary** for the purposes of establishing, exercising or defending legal rights.

8 The processing is **necessary**:

- (a) for the administration of justice;
- (b) for the exercise of any functions conferred by or under any enactment; or
- (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(The Secretary of State may by order specify cases where this condition is either excluded altogether or only satisfied if further specified conditions are met.)

9 The processing –

- (a) is of sensitive personal data consisting of information as to racial or ethnic origin;
- (b) is **necessary** for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and
- (c) is carried out with appropriate safeguards for the rights and freedoms of individuals. (The Secretary of State may specify by order circumstances in which such processing is, or is not, to be taken as carried out with appropriate safeguards for the rights and freedoms of individuals.)

10 The personal information is processed in circumstances specified by order made by the Secretary of State. The existing “Sensitive Data Order” includes detailed provisions for:

- (1) processing that is in the substantial public interest and is necessary for the prevention or detection of any unlawful act and must necessarily be carried out without the explicit consent of the individual being sought so as not to prejudice those purposes; or
- (2) processing that is:-
  - (i) in the substantial public interest;
  - (ii) is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service; and
  - (iii) is carried out without the explicit consent of the individual because the processing:
    - is necessary in a case where consent cannot be given by the individual, or
    - is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent, or

- must necessarily be carried out without the explicit consent of the individual being sought so as not to prejudice the provision of that counselling, support, advice or other service.
- (3) processing that is in the substantial public interest and is necessary for the discharge of any function which is designed for protecting members of the public against:
- (i) dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person, or
  - (ii) mismanagement in the administration of, or failure in services provided by, any body or association, and
  - (iii) must necessarily be carried out without the explicit consent of the individual being sought so as not to prejudice the discharge of that function; or
- (4) the disclosure of personal information that is:-
- (i) in the public interest and
  - (ii) is in connection with:-
    - the commission by any person of any unlawful act (whether alleged or established), or
    - dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person (whether alleged or established), or
    - mismanagement in the administration of, or failures in the services provided by, any body or association (whether alleged or established)
  - (iii) is for the special purposes as defined in section 3 of the Act (i.e. journalistic, artistic or literary purposes); and
  - (iv) is made with a view to the publication of those data by any person and the data controller reasonably believes that such publication would be in the public interest.
- (5) processing of sensitive personal data consisting of information as to religious beliefs (or other beliefs of similar nature) or physical or mental health or condition where:-
- (i) the processing is necessary for identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons with a view to enabling such equality to be promoted or maintained; and
  - (ii) it does not support measures or decisions relating to a individual otherwise than with the individual's explicit consent; and
  - (iii) it does not cause nor is likely to cause substantial damage or distress to the individual or any other person.

The individual has the right to prevent such processing by notice in writing to the data controller.

- (6) processing of personal information consisting of information as to the individual's political opinions that is carried out by certain people or political organisations where it does not cause nor is likely to cause substantial damage or substantial distress to the individual or any other person.

Again, the individual has the right to prevent such processing by notice to the data controller.

- (7) processing that
  - (i) is in the substantial public interest;
  - (ii) is necessary for research purposes (as defined in section 33 of the Act);
  - (iii) does not support measures or decisions with respect to any particular individual otherwise than with the explicit consent of the individual;
  - (iv) does not cause nor is likely to cause, substantial damage or substantial distress to the individual or any other person.
- (8) processing of certain sensitive personal data where the processing is necessary for carrying on insurance business or establishing or administering an occupational pension scheme.
- (9) processing that is necessary for the exercise of any functions conferred on a constable by any rule of law.

### Part 3 – Health, Social Work and Education – Data Protection Orders

This Part 3 concerns where an individual makes a request (a “**Subject Access Request**”) (see paragraph 11 of Appendix 2 to this Protocol) to have access to personal information held about himself or herself or someone for whom he or she has parental or court appointed responsibility.

If any of the information requested consists of certain records or reports relating to the physical or mental health or condition of an individual, or social work, or educational records there are special rules regarding subject access and third party information.

These rules are set out in The Data Protection (Subject Access Modification)(Health) Order 2000 (S.I. No. 413) and The Data Protection (Subject Access Modification)(Social Work) Order 2000 (S.I. No. 415) and The Data Protection (Subject Access Modification)(Education) Order 2000 (S.I No 414).

There follows a brief description of the main points of the three Orders.

#### Health Information

1. If the personal information requested under a Subject Access Request consists of information about the physical or mental health or condition of the individual to whom the personal information relates (“**the Data Subject**”), there is an exemption from complying with that Subject Access Request to the extent that complying would be likely to cause serious harm to the physical or mental health or condition of either:
  - (a) the Data Subject; or
  - (b) any other person.
2. However, a data controller who is not a health professional (as defined in The Data Protection (Subject Access Modification)(Health) Order 2000 (S.I. No. 413)) **shall not withhold** personal information from disclosure under a Subject Access Request on the ground of the exemption described in paragraph 1 above unless the data controller has first consulted the “appropriate health professional” (also defined in the Order) on whether or not that exemption applies.
3. But paragraph 2 above will not apply if the data controller already has a written opinion from the appropriate health professional obtained within the previous six months that the exemption described in paragraph 1 above applies, unless it is reasonable in all the circumstances to re-consult the appropriate health professional.
4. Moreover, a data controller who is not a health professional **shall not disclose** under a Subject Access Request personal information consisting of information as to the physical or mental health or condition of the Data Subject unless:
  - (a) the data controller has first consulted the appropriate health professional on whether or not the exemption described in paragraph 1 above applies;
  - (b) the data controller has previously consulted the appropriate health professional and received an opinion that the exemption described in paragraph 1 above does not apply; or

- (c) the data controller is satisfied that the Data Subject has already seen the information or already knows it.
5. Where the personal information being requested under a Subject Access Request includes information as to the physical or mental health or condition of the Data Subject and:
- (a) (except in relation to Scotland) the Data Subject is a child and the request is made by someone with parental responsibility for the Data Subject; or
  - (b) in relation to Scotland, the Data Subject is a person under 16 and the request is made by someone with parental responsibility; or
  - (c) the Data Subject is incapable of managing his or her own affairs and the person making the request has been appointed by a court to manage those affairs,

the Subject Access Request does not have to be complied with to the extent that it would disclose:

- (d) information provided by the Data Subject in expectation that it would not be disclosed to the person making the Subject Access Request (unless the Data Subject has since expressly indicated that he or she no longer has that expectation); or
  - (e) information resulting from an examination or investigation to which the Data Subject consented in the expectation that it would not be so disclosed (unless the Data Subject has since expressly indicated that he or she no longer has that expectation); or
  - (f) information that the Data Subject has expressly indicated should not be so disclosed.
6. Access to a record containing information as to the Data Subject's physical or mental health or condition cannot be denied on the grounds that the identity of a third party would be disclosed if the third party is a health professional (as defined) who has compiled, or contributed to, the health record or has been involved in the care of the Data Subject in his capacity as a health professional, though that health professional can apply to the court to prevent access on the ground that serious harm to that health professional's physical or mental health or condition is likely to be caused by giving access.

#### Social Work Information

7. If the personal information requested under a Subject Access Request consists of certain social work related information within any of the categories listed in the Schedule to The Data Protection (Subject Access Modification)(Social Work) Order 2000 (S.I. No. 415), there is an exemption from complying with that Subject Access Request to the extent that complying would be likely to prejudice the "carrying out of social work" (which is defined in the Order) by reason of the fact that serious harm would be likely to be caused to the physical or mental health or condition of either:
- (a) the Data Subject; or

- (b) any other person,

but this exemption does not disapply the more limited right of the Data Subject referred to in paragraph 11(a) of Appendix 2 to this Protocol.

8. Where the personal information being requested under a Subject Access Request includes certain social work related information within any of the categories listed in the Schedule to the social work Order and:

- (a) (except in relation to Scotland) the Data Subject is a child and the request is made by someone with parental responsibility for the Data Subject; or
- (b) in relation to Scotland, the Data Subject is a person under 16 and the request is made by someone with parental responsibility; or
- (c) the Data Subject is incapable of managing his or her own affairs and the person making the request has been appointed by a court to manage those affairs,

the Subject Access Request does not have to be complied with to the extent that it would disclose:

- (d) information provided by the Data Subject in expectation that it would not be disclosed to the person making the Subject Access Request (unless the Data Subject has since expressly indicated that he or she no longer has that expectation); or
- (e) information resulting from an examination or investigation to which the Data Subject consented in the expectation that it would not be so disclosed (unless the Data Subject has since expressly indicated that he or she no longer has that expectation); or
- (f) information that the Data Subject has expressly indicated should not be so disclosed.

9. Access to a record containing certain social work related information within any of the categories listed in the Schedule to the social work Order cannot be denied on the grounds that the identity of a third party would be disclosed if the third party is a "relevant person" (as defined in the Order), though that relevant person can apply to the court to prevent access on the ground that serious harm to that relevant person's physical or mental health or condition is likely to be caused by giving access.

#### Educational Records

10. If the personal information requested under a Subject Access Request consists of an educational record (as defined in the DPA 1998), there is an exemption from complying with that Subject Access Request to the extent that complying would be likely to cause serious harm to the physical or mental health or condition of either:

- (a) the Data Subject; or
- (b) any other person.

11. Where the personal information being requested under a Subject Access Request includes personal information consisting of information as to whether the Data Subject is or has been the subject of or may be at risk of “child abuse” (as defined in the Order) and:

- (a) the Data Subject is a child and the request is made by someone with parental responsibility for the Data Subject; or
- (b) the Data Subject is incapable of managing his or her own affairs and the person making the request has been appointed by a court to manage those affairs,

the Subject Access Request does not have to be complied with to the extent that complying with it would not be in the interests of that Data Subject.

12. Access to a record containing an educational record cannot be denied on the grounds that the identity of a third party would be disclosed if the third party is a “relevant person” (as defined in the Order), though that relevant person can apply to the court to prevent access on the ground that serious harm to that relevant person’s physical or mental health or condition is likely to be caused by giving access.

## APPENDIX 6

### PARTIES TO THE AGREEMENT - ADDRESSES, CONTACTS & SIGNATURES

<b>Organisation</b>	
<b>Address</b>	
<b>Contact Details</b>	
<b>Signature</b>	
<b>Name:</b>	
<b>Designation:</b>	
<b>Date:</b>	

<b>Organisation</b>	
<b>Address</b>	
<b>Contact Details</b>	
<b>Signature</b>	
<b>Name:</b>	
<b>Designation:</b>	
<b>Date:</b>	

<b>Organisation</b>	
<b>Address</b>	
<b>Contact Details</b>	
<b>Signature</b>	
<b>Name:</b>	
<b>Designation:</b>	
<b>Date:</b>	

(NOTE all but signature to be completed in block capitals)

SIGNATORY SHEET – SHEET NUMBER \_\_\_\_ OF \_\_\_\_