



haringey strategic partnership

Haringey Safeguarding Adults Multi Agency Information Sharing Protocol

Status: Final

Version: 2.0

Date: September 2009

Foreword:

The effective and timely sharing of information is essential to deliver high quality services focussed on the needs of the individual. In Haringey, we encourage a culture where information is shared with confidence as part of routine service delivery. Sharing information is vital to prevent and detect crime and to ensure that our residents are protected from suffering harm from abuse or neglect.

This Information Sharing Protocol (ISP) explains the terms under which partner organisations have agreed to share information and the practical steps that need to be taken to ensure compliance with those terms. Partner Organisations are fully committed to share information and have agreed to comply with the procedures as set out in this protocol.

The absence of a protocol should not prevent sharing information. If you need to share information outside of the terms of this protocol or with agencies that are not party to this protocol you should follow the guidance as outlined in Haringey's *Simple Guide to Sharing Information* (see appendix E).

The guiding rule is: if you need to share information in order to protect someone from harm or criminal activity, you must do so.

An information sharing guide for practitioners working with vulnerable adults accompanies this protocol. The guide should be given to all relevant staff.

CONTENTS PAGE

Sections:

1. Purpose
2. Background
3. Types of information
 - Personal information
 - Depersonalised information
 - Non-personal information
4. Consent
5. Sharing information without consent
 - Legitimate purpose
 - Public interest
6. Requesting Information under this protocol
7. Disclosing information under this protocol
8. Data Protection
 - Fair processing
 - Retention periods
 - Data quality
 - Security
 - Subject Access Request
9. Freedom of Information
10. Review & Audit
11. Key legislation
 - Crime and Disorder Act 1998
 - National Health Service Act 2006
 - National Health Service and Community Care Act 1990
 - No Secrets: Guidance on developing Multi-Agency Policies and Procedures to Protect Vulnerable Adults from Abuse

List of Appendices

- A – Parties to the protocol
- B – Glossary of terms
- C – Request/Disclosure and Consent forms
- D - Additional legislation relating to this protocol
- E – Simple Guide to information sharing
- F - Caldicott principles
- G - Procedure document for PCT and ACS use of Framework-i for the Single Assessment Process, and associated common activity

Document Control

Issue	Date	Author	Comments	Approval
1.0		Stephen Cornell	Initial Draft	
1.1	03/10/03	Stephen Cornell	Revisions to Indemnity	
1.2	08/08/06	ISP- ASWG/Sophie Johnson	Initial Adult Draft	
1.3	12/12/06	ISP- ASWG/Sophie Johnson	Initial Adult Draft – Minor Amendments	
1.4	22/02/07	ISP- ASWG/Sophie Johnson	Initial Adult Draft – Updated format	
2.0	24 September 2009	Anita Hunt/Richard Kaufman	Revised document	Well-being Strategic Partnership Board

This protocol became effective on 24 September 2009.

This protocol will be reviewed annually – please refer to Section 10 of this document (Review and Audit).

Any significant amendments to this protocol made before the review date stated above will need to be approved in principle by all Partner Organisations and will only be effective until the review date. All significant amendments will need to be endorsed by the Partner Organisations at the review date.

1. Purpose

- 1.1 This Information Sharing Protocol (ISP) is an agreement between Partner Organisations (see appendix A for a list of parties to this protocol) specifically to facilitate and govern information sharing. Its purpose is:
 - to facilitate the secure exchange of information, where necessary to ensure the health, well-being and safeguarding of Adults in Haringey.
 - to provide a framework for the secure and confidential sharing of personal information between the partner organisations.
- 1.2 For the purposes of this protocol, an individual may be referred to as a patient, client or data subject.
- 1.3 ISPs are not required before front-line practitioners can share information about an individual. By itself, the lack of an ISP must never be a reason for not sharing information that could help a practitioner deliver services to an individual.

2 Background

- 2.1 The sharing of personal information between organisations is vital to ensure co-ordinated and seamless provision of services that are protective and supportive. Sharing information will:
 - Provide professionals with background information on a named person
 - Reduce the need for information to be repeated to different professionals
 - Enable professionals to keep track of their interventions and the status of their contact with the named person
 - Ensure that the named person can be traced
 - Identify individuals who have not benefited from service support in the past
 - Reduce duplication of data collection across partner agencies
 - Improve the consistency and accuracy of management information
 - Progress assessment and care planning on a multi-agency/professional basis
- 2.2 The *No secrets* guidance was issued in 2000, as guidance under section 7 of the Local Authority Social Services Act 1970. It created, for the first time, a framework for multi-agency action in response to the risk of abuse or harm. *No secrets* recognised that some forms of abuse are criminal offences, and that police investigations are required and appropriate.
- 2.3 Practitioners working in adults' services are aware that problems faced by clients who have parenting responsibilities, are often likely to affect children

and other family members, for example: vermin, alcohol and drugs or where there is a dangerous weapon in the house. However this information is not always shared and opportunities to put preventative support in place for the children and family are missed. Where an adult receiving services is a parent or carer, sharing information where appropriate with colleagues in children's services could ensure that any additional support required for their children can be provided early.

3 Types of information

3.1 Personal information

- 3.1.1 The Data Protection Act 1998 defines 'personal information' as information relating to a living individual who can be identified either from that information or from that information in conjunction with other information that is in, or is likely to come into, the possession of the data controller.
- 3.1.2 A person's full name is an obvious likely identifier; but other information such as a customer reference number, address, photograph or CCTV image could also identify them.
- 3.1.3 The definition of personal information is technology neutral; it does not matter how the information is stored (e.g. on a computer database, paper filing system, microfiche, portable memory stick).
- 3.1.4 Where it is necessary for information to be shared, personal information will be shared only on a need-to-know basis.
- 3.1.5 Any duty of confidentiality will be respected unless there is an overriding 'public interest' to disclose the information and if there is a 'legitimate purpose' to sharing (see section 5). Where the disclosure would breach client confidentiality the request should be referred to a designated manager - unless exceptional circumstances apply, e.g. where there is a need for urgent medical treatment. Managers should have access to a source of advice and support on information sharing issues. This may be a Caldicott Guardian. In the absence of advice from their own agency officers and/or managers should contact: Head of Service-Adult Protection on 0208 489 3106.
- 3.1.6 The reasons for breaching client confidentiality must be fully recorded and clearly referenced to the evidence and information on which the decision is based. This must include details of any third parties and details of all the information/evidence they have been given.

3.2 Depersonalised information

- 3.2.1 Depersonalised information encompasses any information that does not and cannot be used to establish the identity of a living person, having had all identifiers removed.
- 3.2.2 Partner Organisations accept that there are no legal restrictions on the exchange of depersonalised information, although a duty of confidence may apply in certain circumstances, or a copyright, contractual or other legal restriction may prevent the information being disclosed to Partner Organisations.
- 3.2.3 Information shared between Partner Organisations should be limited for the purposes of the enquiry. If the purpose of this protocol can be achieved using depersonalised information, then this should be the preferred method used by officers. For example, in assessing crime hotspots geographic information that does not identify living individuals might be used for strategic planning purposes.
- 3.2.4 Partner Organisations recognise that great care must be taken when depersonalising information and that the Information Commissioner has stated that even a post-code or address can reveal the identity of an individual. Partner Organisations are also aware that it may be possible for an individual's identity to be revealed by comparing several sets of depersonalised data.

3.3 **Non-personal information**

- 3.3.1 Partner Organisations understand that non-personal information is information that does not, nor has ever, referred to individuals.

4 **Consent**

- 4.1 Many issues surrounding the disclosure of personal information can be avoided if the consent of the individual has been sought and obtained. Obtaining consent remains a matter of good practice and in circumstances where it is appropriate and possible, informed consent should be sought. (There is a 'Consent Form' at appendix C of this protocol that can be used if signed consent has not already been obtained as part of the assessment or referral process).
- 4.2 Practitioners should encourage clients to see information sharing (and giving their consent to share their personal information) in a positive light, as something which makes it easier for them to receive the services that they need.
- 4.3 **Whose consent to seek:**

- 4.3.1 All people aged 16 and over are presumed, in law, to have the capacity to give or withhold their consent to sharing of confidential information, unless there is evidence to the contrary. If an adult lacks the capacity to take their own decisions, then professionals should share information that is in their 'best interests'. A 'best interests' checklist is set out in section 4 of The Mental Capacity Act 2005 http://www.opsi.gov.uk/acts/acts2005/ukpga_20050009_en_1. The Act provides a statutory framework to empower and protect vulnerable people who may not be able to make their own decisions. It makes it clear who can take decisions in which situations and how they should go about this. The Act defines the term 'a person who lacks capacity' as a person who lacks capacity to make a particular decision or take a particular action for themselves, at the time the decision or action needs to be taken.
- 4.3.2 In recent years, the subject of undue influence has received increasing attention in the field of elder abuse prevention. Simply stated, undue influence is when an individual who is stronger or more powerful gets a weaker individual to do something that the weaker person would not have done otherwise. For example, the stronger may isolate the weaker person, promote dependency, or induce fear and distrust of others. Because undue influence (like mental capacity) raises the question of whether an individual is acting freely, the two concepts are often confused. Although diminished mental capacity may contribute to a person's vulnerability to undue influence, the two are distinct and cognitive assessments cannot identify the presence of undue influence. It is typically courts that make determinations of whether or not undue influence has been exercised. In doing so, they consider a variety of factors, including whether the transaction took place at an appropriate time and in an appropriate setting and whether the older person was pressured into acting quickly or discouraged from seeking advice from others. Courts also consider the relationship between the parties, and the "fairness" of the transaction.

5 Sharing information without consent

- 5.1 Practitioners should not seek consent when they are required by law to share information through a statutory duty or by a court order. Consent should also not be sought if doing so would:
- place a person (the individual, family member, staff or a third party) at increased risk of significant harm if a child, or serious harm if an adult; or
 - prejudice the prevention, detection or prosecution of a serious crime; or
 - lead to an unjustified delay in making enquiries about allegations of significant harm to a child, or serious harm to an adult.

- 5.1.1 An example of where not sharing information could place a person at increased risk of significant harm, is in a situation where a vulnerable member of the public requires urgent medical assistance and information is not shared between partner agencies. In emergency medical situations information should always be shared between partner agencies. In circumstances where vulnerable members of the public carry emergency alert cards, the instructions on the card should be followed in line with service procedures.
- 5.1.2 If consent has not been sought, or sought and withheld, the agency must consider if there is a 'legitimate purpose' for sharing the information and if it is in the 'public interest' to share.
- 5.2 Consent lasts as long as co-ordinated inter-agency services are required, unless it is withdrawn. Individuals have the right to withdraw consent after they have given it.

5.3 **Legitimate Purpose**

5.3.1 Partner Organisations understand the 'Legitimate Purpose' criteria to include:

- Preventing serious harm to an adult - including through prevention, detection and prosecution of a serious crime.
- Providing urgent medical treatment to an adult.
- Implementing the Department of Health's 'No Secrets' agenda – which aims to protect vulnerable adults from abuse.

5.4 **Public Interest**

5.4.1 Partner Organisations understand the 'Public Interest' criteria to include:

- When there is evidence or reasonable cause to believe that an adult is suffering, or it at risk of suffering, serious harm;
- To prevent the adult from harming someone else;
- The promotion of welfare of the adult;
- Detecting crime;
- Apprehending Offenders;
- Maintaining public safety; and
- Administration of justice

- 5.4.2 When considering whether disclosure is in the public interest, the rights and interests of the individual must be taken into account. A fair balance between the public interest and the rights of the individual must be ensured.

6 Requesting Information under this protocol

- 6.1 Where staff have reasonable cause to believe that an adult may be at risk of suffering serious harm, they should always consider referring their concerns to social services or to the local police force – in line with the Safeguarding Adults Board (SAB) Policies and Procedures. In some situations staff may be unsure whether ‘a concern’ that an adult may be at risk of suffering serious harm, constitutes ‘a reasonable cause to believe’. In these situations, the concern must not be ignored. When in doubt, staff should always talk to a lead person on safeguarding to help them decide what to do – for example: their manager or an experienced and trusted colleague. If those officers are in doubt, then they should speak to a Caldicott Guardian. Staff should try to protect the identity of the individual (wherever possible), until they have established a reasonable cause for their belief.
- 6.2 Where staff need information from a Partner Organisation party to this protocol they should submit their inquiry in writing using the ‘Request/Disclosure’ form found in appendix C of this protocol.
- 6.3 Where appropriate, the requesting officer must also supply the Partner Organisation with evidence of the client’s consent. (for more information on ‘Consent’ see section 4).
- 6.4 The ‘Request/Disclosure’ form must be added to the client’s record.
- 6.5 The requesting and disclosing officers will ensure that any personal information is transferred in secure manner (for more information on ‘Security’ see section 8.5)
- 6.6 Routine exchanges of information, such as asking whether a person is known to a service, should be requested formally (and agreed by the supplying partner) on one form. There is no need to submit a separate form for each occurrence. Such procedure is subject to a continued review by participating Partner Organisations and by a further formal request form every 9 months if de-personalised or non-personal or 6 months if personal.

7 Disclosing Information under this protocol

- 7.1 Staff disclosing information must always consider the safety and welfare of the client when making decisions on whether to share information about them. For example, where there is concern that an adult may be suffering or is at risk of suffering serious harm, then the adult’s safety and welfare must be the overriding consideration.

7.2 Officers disclosing information must ensure that the requesting officer has supplied a completed 'Request/Disclosure' form and, where appropriate, evidence of the client's consent (for more details on 'Consent' see section 4).

7.3 The disclosing officer must also ensure that any information disclosed is:

- necessary for the purpose for which they are sharing it;
- accurate and up-to-date;
- depersonalised (where appropriate);
- shared only with those people who need to see it; and
- transferred securely.

7.4 The disclosing officer must complete the appropriate section of the 'Request/Disclosure' Form and save it in line with service procedures.

8 Data Protection

8.1 Data Protection Act

8.1.1 Partner Organisations agree to comply at all times with data protection legislation and other legal requirements relating to confidentiality.

8.2 Fair Processing

8.2.1 The Data Protection Act 1998 requires that when personal information is collected from a data subject, they are told what it will be used for and who the information will be shared with. When collecting information from clients, staff in partner organisations should explain:

- What is done with the information;
- The reason why professionals are capturing it; *and*
- Who the information can be routinely shared with

8.2.2 Partner Organisations will ensure that their 'Fair Processing Notices' are kept up-to-date and provide an accurate explanation of the information sharing activities that are being undertaken.

8.3 Retention Periods

8.3.1 All partner organisations who are party to this protocol will put in place policies and procedures governing the retention and destruction of records containing personal information retained within their systems.

8.3.2 As a general rule, partner organisations agree that personal information that has been shared will be destroyed once it no longer is of relevance to the initial inquiry.

8.4 Data Quality

8.4.1 Partner organisations will notify the source of the information if they discover that the information is inaccurate or inadequate for the purpose. The source will be responsible for correcting the data and notifying all other recipients in writing.

8.5 Security

8.5.1 Personal information will be kept securely within a computer system or otherwise physically secure with appropriate levels of staff access in line with party organisations' information security policies and procedures. These policies and procedures should be based on national standards and guidance

8.5.2 Staff in Partner Organisations involved in information sharing under this protocol must:

- Be fully aware of their responsibilities under the protocol mentioned above, together with the Data Protection Act and Duty of Confidentiality.
- Use information only for the purpose stated in the original request for information.
- First obtain consent from the disclosing organisation, if they wish to pass the information onto a third party. (In a high risk situation involving safeguarding, this may not always be a reasonable requirement. In emergencies, the public interest disclosure is a sufficient exemption to override this requirement).
- Store hard copies of the request/disclosure and consent forms in a lockable container when not in use, and a clear desk policy implemented.
- If the information is held electronically, access must be restricted only to persons with a genuine 'need to know' the information.
- Once this information is no longer required, it must be destroyed. Only the minimum amount of personal information should be retained which is necessary to achieve the purpose for which it was obtained.

8.6 Each Partner Organisation is responsible for ensuring that the appropriate staff are adequately trained in respect of all matters covered by this protocol. All temporary and agency staff will be appropriately briefed on their responsibilities as part of their induction.

8.7 Subject Access Requests

- 8.7.1 The Data Protection Act gives people the right to apply to an organisation that holds personal information about them for access to that information. The exercise of this right is referred to as a subject access request. People may exercise this right on their own behalf or through a representative. Where people do not have the mental capacity to make a request on their own behalf, because they are too young or for some other reason, their parent or person with Power of Attorney may make the request on their behalf. All partner organisations that are party to this protocol will put in place procedures for handling requests for personal information.
- 8.7.2 The right of subject access applies to all personal information held by an organisation about that data subject regardless of whether or not that organisation is the “owner” or “source” of the information. The information must be disclosed to the data subject unless one of the exemptions in the Data Protection Act applies. It may be appropriate for the organisation that has received the subject access request to consult with the source of the information they hold to discuss whether the information is subject to an exemption.

9 Freedom of Information

- 9.1 The Freedom of Information Act 2000 (FOI) enables any member of the public to apply for access to information held by bodies across the public sector. The Act provides a general right of access to information held by public authorities in the course of carrying out their public functions, subject to some exemptions. This right does not extend to personal information, which is largely exempt from the Freedom of Information Act.
- 9.2 Partner Organisations will ensure that this protocol is included in their Publication Scheme.

10 Review and Audit

- 10.1 The protocol will be reviewed by the Partner Organisations annually.
- 10.2 The review is to be undertaken jointly by officers agreed by the Partner Organisations unless agreed by the Partner Organisations for a single Partner Organisation to undertake the review. This work will be coordinated by the Adult Safeguarding Board. At each review date the respective board will pull together a review group made up of parties to the protocol, and identify operational problems, new legislation and highlight any proposed amendments to be agreed.
- 10.3 Partner Organisations may audit compliance with this protocol.
- 10.4 Partner Organisations agree to assist other Partner Organisations during the audit process as long as reasonable notice is given in writing detailing the scope of the audit process and they do not object.

11 Key Legislation

- 11.1 The Key pieces of legislation that expressly authorise information sharing relating to the safeguarding of children are:

11.2 **Crime and Disorder Act 1998**

- 11.2.1 http://www.opsi.gov.uk/acts/acts1998/ukpga_19980037_en_1

Disclosure may be made despite a duty of confidentiality where there is an overriding public interest, for example to prevent or detect crime, disorder, anti-social behaviour, annoyance/ nuisance, dwellings being used for immoral or illegal purposes.

- 11.2.2 The exchange of personal information post conviction will be subject to the same presumption of confidentiality. However, the administration of justice and the prevention of crime are in the public interest and will provide the grounds upon which a disclosure can be justified. Care must be exercised in the disclosure of conviction data. In this case it must support action under the Crime and Disorder Act and a Designated Officer must ensure that the information is accurate and relevant to an enquiry before it is released.

11.3 **National Health Service Act 2006**

- 11.3.1 http://www.opsi.gov.uk/acts/acts2006/ukpga_20060041_en_1

Part 3 Section 82, of the National Health Service Act 2006 places a duty on NHS bodies and local authorities to co-operate with one another in order 'to secure and advance the health and welfare of the people of England and Wales'.

11.4 **National Health Service and Community Care Act 1990**

11.4.1 http://www.opsi.gov.uk/ACTS/acts1990/ukpga_19900019_en_1

Provides that when a local authority is assessing need and it appears that there may be a need for health or housing provision, the local authority shall notify the appropriate PCT, Health Authority or housing department and invite them to assist.

11.5 ***No Secrets: Guidance on developing Multi-Agency Policies and Procedures to Protect Vulnerable Adults from Abuse***

11.5.1 www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4008486.

This document states that the government expects organisations to share information about individuals who may be at risk from abuse.

List of Appendices

A – Parties to the protocol

B – Glossary of terms

C - Consent form

D - Additional legislation relating to this protocol

E – Simple guide to information sharing

F - Caldicott principles

G - Procedure document for PCT and ACS use of Framework-i for the Single Assessment Process, and associated common activity

Appendix A – Parties to the protocol

Organisation	Representative
Haringey Council	Lisa Redfern Caldicott Guardian
Homes for Haringey	Paul Bridge Chief Executive
NHS Haringey	Tracey Baldwin Chief Executive
Great Ormond Street Hospital	Dr Jane Collins Chief Executive
Metropolitan Police Service (Haringey Division)	David Grant Borough Commander
North Middlesex University Hospital	Clare Panniker Chief Executive
Whittington Hospital	Dr Clarissa Murdoch Caldicott Guardian
BEH Mental Health Trust	Lee Botjor Director of Governance and Caldicott Guardian
CAFCASS	Elizabeth Hall Regional Manager
London Probation – Area Haringey	Mary Pilgrim Head of Service Delivery
HAVCO	Naeem Sheikh Chief Executive
Learning and Skills Council	Yolande Burgess Partnership Director
College of North east London (CONEL)	Paul Head Principal & Chief Executive
Middlesex University	Lucille Allain Director of Social Programmes
Haringey Fire Service	John Brown Borough Commander Haringey

Appendix B: Glossary

Caldicott Guardian is a person with responsibility for policies that safeguard the confidentiality of patient information.

Confidential is information that has a degree of sensitivity and value and is subject to a duty of confidence.

Consent is when someone accepts or agrees to something that somebody else proposes. For consent to be legal and proper, the person consenting needs to have sufficient mental capacity to understand the implications and ramifications of his or her actions.

Information Sharing Protocol (ISP) - is a signed agreement between two or more partner organisations relating to a specified information sharing activity. An ISP explains the terms under which the organisations have agreed to share information and the practical steps that need to be taken to ensure compliance with those terms.

Practitioner is the generic term used in this guidance to cover everyone who works with children and young people.

Public interest is the interests of the community as a whole, or a group within the community or individuals.

Serious harm for the purposes of this guidance can be either physical or mental trauma to an adult.

Significant harm – there are no absolute criteria on which to rely when judging what constitutes significant harm. Consideration of the severity of ill treatment may include the degree and the extent of physical harm, the duration and frequency of abuse and neglect, the extent of premeditation, and the presence or degree of threat, coercion, sadism, and bizarre or unusual elements.

Well-being has a legal definition based on the five *Every Child Matters* outcomes; the achievement of these outcomes is in part dependent upon the effective work to safeguard and promote the welfare of children, young people and families.

Appendix C: Safeguarding Adults Multi-Agency Information Sharing Protocol - Request/Disclosure Form

Requesting Officer's Ref:	
Disclosing Officer's Ref:	

PART A – INFORMATION REQUESTED - (to be completed by requesting officer)

Information requested by:

Name:	
Organisation/Department:	
Contact phone number:	
Email address:	

Information requested:

Describe the information required and the circumstance that have led to this request being made, including any names, addresses and dates of birth.

--

Name:	
Address:	
DOB (ddmmyy):	
NHS Number	

Date information is required by (ddmmyyyy):	
If urgent, please state reason:	

Have you obtained consent to share information? (Please ensure that you attached the standardised 'Consent Form').		
If consent has not been obtained from the individual, please indicate for what purpose you require this information? (Please tick the relevant boxes as appropriate)		
Preventing serious harm to an adult – <input type="checkbox"/> <i>including through prevention, detection and prosecution of a serious crime.</i>	Providing urgent medical treatment to an adult <input type="checkbox"/>	Implementing the Department of Health's 'No Secrets' agenda – <input type="checkbox"/> <i>which aims to protect vulnerable adults from abuse.</i>
In the 'public interest' and a 'legitimate purpose' to share <input type="checkbox"/> <i>(for more information see section 5 of Haringey's Safeguarding Adults Multi-</i>	There is a statutory obligation or court order to share <input type="checkbox"/>	Please provide details:

<i>Disciplinary Information Sharing Protocol (ISP)</i>	
--	--

Signature of requesting officer:		Date:			
----------------------------------	--	-------	--	--	--

PART B - INFORMATION DISCLOSED – (to be completed by disclosing officer)

Disclosure Agreed:	Yes <input type="checkbox"/> No <input type="checkbox"/>
Information attached to this form	Yes <input type="checkbox"/> No <input type="checkbox"/>
Reason for declining request (if applicable):	

Information disclosed (Continue on a separate sheet if necessary, and remember to attach any additional sheets to this form)	
---	--

Information disclosed by:

Name:	
Department /Organisation:	
Contact phone number:	
Email address:	

Delivery method (please mark as appropriate): Email Fax Other (please specify)

Signature of disclosing officer: _____ Date supplied: _____

Consent Form

Haringey's Safeguarding Adults Multi-Agency Information Sharing Protocol - Consent Form

Requesting Officer's Ref:	
Disclosing Officer's Ref:	

Please provide the relevant information below:

Is this information about you?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If 'No', who is the information about?		
Name:		
Address:		
DOB (ddmmyyyy)		
Are you are acting as: Parent/Guardian/Carer Other (please describe)		

Have the reasons for requesting consent been explained to you?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
--	------------------------------	-----------------------------

I give:	
consent to disclose to:	

Information to which this consent applies:

Personal information and any relevant information, for the purposes of:

Your Name:			
Address:			
DOB (ddmmyyyy):			

Signature:			
Date (ddmmyyyy):			

Witnessed by requesting officer:

Name:			
Position:			
Signature:			
Date (ddmmyyy):			

Appendix D: Additional legislation relating to this protocol

The principles and procedures embodied in this protocol are underpinned by the following legislation not outlined in the 'Key Legislation' section of this protocol:

- . European Convention on Human Rights (given effect via the Human Rights Act 1998)
- . Data Protection Act 1998
- . Freedom of Information Act 2000
- . Common Law Duty of Confidentiality
- . Regulation of Investigatory Powers Act 2000
- . Access to Health Records Act 1990
- . Community Care (Delayed Discharges) Act 2003
- . National Health Service and Community Care Act 1990
- . Health and Social Care Act 2001
- . Health Act 1999
- . The Children Act 1989
- . The Local Government Act 2000
- . The Education Act 1996
- . The Education Act 2002
- . The Learning and Skills Act 2000
- . Children (Leaving Care) Act 2000
- . Education (SEN) Regulations 2001
- . NHS Bodies and Local Authorities Partnership Arrangements Regulations 2000
- . The NHS (Venereal Diseases) Regulations 1974 and NHS Trusts (Venereal Diseases) Regulations 1991
- . The Abortion Regulations 1991
- . The Human Fertilisation and Embryology Act 1990
- . *Working Together to Safeguard Children* (HMG, 2006),
- . Education and Inspections Act 2006
- . Child Health Promotion Programme (DH, 2008)

Non-legislation includes;

- . Caldicott Guidelines
- . Local codes or standards relating to confidentiality
- . Local Policies and Procedures around Haringey's Local Safeguarding Children's Board (LSCB) and Haringey's Local Safeguarding Adults Board (LSAB)

Appendix E: Simple Guide to information sharing

Information sharing with consent

If you have the person's consent, then it is ok to share personal information about them. Obtaining explicit consent for information sharing is best practice in most situations but it is not always possible or appropriate to do so.

Information sharing protocols

An Information Sharing Protocol (ISP) is a signed agreement between two or more organisations relating to a specified information sharing activity. An ISP explains the terms under which the organisations have agreed to share information and the practical steps that need to be taken to ensure compliance with those terms. If there is an ISP applicable to your information sharing situation, you must follow that. ISPs are not required for information sharing. The absence of an ISP should not prevent sharing information.

The Golden Rules¹ for information sharing

Where you are considering sharing information and you do not have the person's consent and there is not an information sharing protocol in place to govern that exchange of information; following the golden rules should ensure that you strike the correct balance between protecting people's privacy and ensuring that fellow practitioners have the information they need to deliver services.

1. Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.

2. Be open and honest with the person from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

¹ The Golden Rules have been copied from "Information Sharing: Guidance for practitioners and managers" published by the Department for Children, Schools and Families, and Communities and Local Government.

5. Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Appendix F - Caldicott principles

1. Justify the purpose(s)

Every proposed use or transfer of identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use identifiable information unless it is absolutely necessary

Identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for subjects to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary identifiable information

Where use of identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4. Access to identifiable information should be on a strict need-to-know basis

Only those individuals who need access to identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

5. Everyone with access to identifiable information should be aware of their responsibilities

Action should be taken to ensure that those handling identifiable information are made fully aware of their responsibilities and obligations to respect confidentiality.

6. Understand and comply with the law

Every use of identifiable information must be lawful. Someone in each organisation handling information should be responsible for ensuring that the organisation complies with legal requirements.

Appendix G – Procedure document for PCT and ACS use of Framework-i for the Single Assessment Process, and associated common activity

The purpose of this protocol is to enable approved use of Framework-i as a client record tool and authorised information sharing vehicle between London Borough of Haringey in its role as a Council with Social Services Responsibility and the Haringey Primary Care Trust.

It is not practical or desirable to create an environment of highly restricted access to information, as this would defeat the information sharing objective, and could increase risk to vulnerable clients. However, there is a need to safeguard against unauthorised use.

It is recognised that staff in both the PCT and LB Haringey are subject to agency confidentiality policies, record keeping policies and policies on use of computers and IT systems, and that breach of these policies and procedures could give rise to invocation of the parent agency's disciplinary procedures.

The Framework system provides an audit capability to identify, by user ID, the records accessed and the type of access activity undertaken and date and time of the activity. This would facilitate an underpinning safeguard.

The proposed information sharing protocol is to adopt the convention of an on-screen warning note - to be created by the person-record initiator/owner, where information sharing agreement has not been given by the client. The proposed text is **“WARNING INFORMATION SHARING CONSENT NOT GIVEN”** – access own agency information only”, which would be displayed on the front – person details screen.

The expectation is that workers should seek to get the FACE/SAP information sharing agreement signed, and once signed, the warning should be removed.

Additional case note classifications of **“Confidential – PCT case note”**; **“Confidential- LBH case note”** are also proposed.

Framework episodes are prefixed by: LBH or PCT to differentiate between the agencies.

It is also proposed that there are ongoing regular Framework usage review meetings between LBH and PCT, and that information sharing should be a core agenda item for these meetings.