Harrow COUNCIL
LONDON

& our Partners,

Committed to
Safeguarding Adults

Harrow's Local Safeguarding Adults Board (L.S.A.B.)

Safeguarding Adults Information Sharing Protocol

An agreement between members and partner organisations of Harrow Council's LSAB to support the sharing of information between all agencies in relation to the prevention, detection or investigation of a Safeguarding Adults concern under Harrow's Safeguarding Adults Policy and Procedures.

www.harrow.gov.uk/safeguardingadults

safeguarding.adults@harrow.gov.uk

020 8420 9453 during office hours or:

020 8424 0999 at all other times

Harrow COUNCIL
LONDON

Seamus Doherty, Safeguarding Adults Co-ordinator, November 2010

CONTENTS

1. Introduction

1.1 Harrow Council and the Local Safeguarding Adults Board (LSAB) recognise that a high profile, transparent information sharing protocol is a key mechanism to ensure that a structured process is in place to facilitate the sharing of information between all partners involved in the Safeguarding Adults process.

1.2 Effective and structured sharing of information between partners has the ability to inform planning, allow for an understanding of trends and patterns of activity to be developed, to respond to emergencies and disasters appropriately, and to intervene and support the lives and safety of individuals, families and communities.

1.3 In a world of increased information gathering and recording, individuals and organisations have a moral and statutory responsibility to share information carefully and responsibly – this document will outline the principles of information sharing and clarify the duties and responsibilities of professionals working within this protocol.

1.4 Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal information is lawful, properly controlled and that an individual's rights are respected. This must however be balanced with the need to share information to provide safe quality services, to protect individuals and the wider public and the protection of those individuals confidentiality.

1.5 Uncertainty over the legal position may lead to information not being readily available to those who have a genuine need to know in order for them to do their job properly and provide the services required to safeguard adults at risk.

1.6 This information sharing protocol (ISP) sets out the principles for using and sharing personal information among the members and member organisations of Harrow's Local Safeguarding Adults Board.

2. Purpose of the Agreement

This ISP has been developed to:

2.1 Set out a framework for partner organisations to manage and share information on a lawful and 'need to know' basis with the purpose of enabling them to meet both their statutory obligations and the needs and expectations of the people they serve.

2.2 Set out the legal framework within which the information is shared, including reference to legal powers to share information, the Human Rights Act 1998, the common law duty of confidentiality, the Data Protection Act 1998, and other relevant legal considerations.

2.3 Define the specific purposes for which the signatory agencies have agreed to share information.

2.4 Describe the roles and structures that will support the exchange of information between agencies.

2.5 Describe the security procedures necessary to ensure compliance with responsibilities under the Data Protection Act and agency specific security requirements.

2.6 Describe how this arrangement will be monitored and reviewed.

2.7 This protocol outlines the principles and standards of expected conduct and practice of the signatories and their staff and applies to all sharing of personal and non-personal information. The Protocol establishes the organisation's intentions and commitment to information sharing and promotes good practice when sharing personal information. It also contains the legislative standards that all types of personal information sharing must comply with.

2.8 This protocol also sets out the detail of what information is to be shared, how it will be shared and who it will be given to. It also sets out the limits to any information sharing and the extent to which it may be passed on to a third party without recourse to the originator of the information.

2.9 The arrangements set out within this protocol cover the sharing of information within a Safeguarding Adults context and does not take the place of or adversely impact on any other information sharing protocols between individual or collective agencies i.e. MAPPA, MARAC, Community Safety etc.

3. What does the protocol cover?

This protocol applies to the following types of data:

3.1 Personal information

3.2 The term 'personal' information refers to any information held either as manual and/or electronic records, or records held by means of audio and /or visual technology, about a living individual who can be personally identified from that information.

3.3 Certain types of personal information have been classified as sensitive data, where additional conditions must be met for that information to be used and disclosed lawfully. The term 'sensitive' data refers to information that provides details of racial or ethnic origin, political opinions, religious beliefs, Trade Union membership, physical or mental health, sexual life, commission or alleged commission of an offence, criminal proceedings or sentence.

3.4 Anonymised information

3.5 Information that falls into this category is data about people that has been aggregated or tabulated in ways that make it impossible to identify the details of individuals. This can be shared without the consent of the individuals involved. However, care should be taken to ensure that it should not be possible to identify individuals either directly or in summation. This can happen when anonymised information is combined with other data from different agencies, where the aggregated results produce small numbers in a sample, or where

traceable reference numbers are used.

3.6 **Non-personal information**

3.7 Information that does not relate to people; e.g. information about organisations, natural resources and projects, or information about people that has been aggregated to a level that is not about individuals.

3.8 There is a general presumption and expectation that anonymised and non-personal information will be shared, unless there are exceptional reasons for this. These may include:

- commercial confidentiality;
- policy formulation (where a policy is under development and circulation would prejudice its development);
- legal prejudice; and
- where information is marked protectively (refer to your organisations standards for information classification for further details in this area)

3.9 This protocol applies (within a Safeguarding Adults context) to all organisations and agencies who are formal or informal members of Harrow's LSAB. This will include all elected members, non-executive members, trustees and all employees of the council and partner organisations.

3.10 **The list below highlights the current membership of the LSAB and the signatories to this protocol, this list is not exhaustive and new members will be asked to sign-up to this protocol as part of their induction to the LSAB. The current agency partners include;**

Harrow Council
Harrow PCT / NHS Harrow
Ealing and Harrow NHS Community Services
North West London Hospital Trust
Royal National Orthopaedic Hospital NHS Trust
Central and North West London Mental Health NHS Foundation Trust
Metropolitan Police
Care Quality Commission
Age Concerns Harrow
Harrow Mencap
Harrow Association of Disabled People
Mind in Harrow
Harrow LINk
Harrow Association of Voluntary Services
Community Link Up
Carers Support Harrow
Supporta Care
Gentle Care
Care UK
Support for Living
Fremantle Trust
Hadley House / Stanmore Residential Home

3.11 This protocol also applies to any organisation or agency which has been commissioned to deliver services on behalf of any organisation party to this protocol where permission has been given to the third party organisation to disclose information or they have a legal duty to do so.

3.12 Organisations will need to bring this protocol to the attention of any 3rd party organisations they work with and they too will be subject to the Data Protection Act in terms of the personal information they process.

3.13 It is also intended to complement existing professional Codes of Practice that apply to any relevant profession working within any signatory or third party organisation.

3.14 It should however be noted that this does not constitute or replace the potential for independent legal or ethical advice.

4. Legal responsibility to share

4.1 The legal framework within which public sector data sharing takes place is complex and overlapping and there is no single source of law that regulates public sector information sharing.

4.2 The purpose here, therefore, is to highlight the legal framework that affects all types of personal information sharing, rather than serve as a definitive legal reference point.

4.3 The principal legislation, guidance and regulations concerning the protection and use of personal information are listed below:

- the Children Act 1989 and 2004
- the Data Protection Act 1998
- the Human Rights Act 1998
- the Crime and Disorder Act 1998
- the Freedom of Information Act 2000
- “No Secrets”, Department of Health 2000
- Regulation of Investigatory Powers Act 2000
- Police Reform Act 2002
- Criminal Justice Act 2003
- Civil Contingencies Act 2004
- Safeguarding Adults, ADSS 2005
- Police and Justice Act 2006
- Working Together to Safeguard Children 2006 Statutory guidance
- Local Government & Public Involvement in Health Act 2007
- the Common Law Duty of Confidence
- the Caldicott Principles
- Children and Young Persons Act 2008

5. Purposes for which the information will be shared

5.1 Information will only be shared for a specific lawful purpose or where appropriate consent has been obtained. The following range of purposes are deemed as justifiable for the transfer of personal information between partner

agencies as defined within the remit of this protocol:

- to ensure that vulnerable adults are given the appropriate care and protection they require to live a life free from abuse, harm or exploitation
- to support a robust assessment to determine whether a vulnerable adult is at risk or likely to be at risk of serious harm so that all relevant information can be evaluated and contribute towards the development of risk assessment and risk management plan
- to ensure that where safeguarding issues have been highlighted or where there are concerns about the care or treatment of a vulnerable adult, that appropriate, timely and robust action can be taken to protect that individual/s from further harm
- for the prevention and detection of crime and / or the promotion of community cohesion and safety
- to allow organisations to cooperate so that they can deliver the required care and support services in situations where safeguarding issues have been highlighted
- to allow organisations to cooperate so that all partners can, at both strategic and operational levels, work in a co-ordinated and joined up way to bring about service improvements, enhance delivery and better meet the needs of those who use those services
- to monitor and protect public health and well being
- to ensure compliance with legal responsibilities e.g. court orders
- for the investigation of complaints or actual / potential legal claims
- to support or contribute towards Serious Case Reviews
- to support an individual or agency in carrying out their statutory duties
- to support the provision of quality local data at appropriate levels so that policy and practice is evidence-led
- to support the planning and commissioning of more efficient, easier to access services
- to support improvements to existing and new services
- to manage, report and benchmark performance
- to promote accountability to customers, stakeholders, local residents and Government
- statistical analysis for research and training
- to enable better co-ordination in promoting and marketing public events across the Borough

6. Restrictions on use of Information Shared

6.1 Information must only be used for the purpose(s) specified at the time of disclosure as defined in the relevant Information Exchange Agreement

6.2 It is a condition of access that it must not be used for any other purpose without the permission of the Data Controller who supplied the data, unless an exemption applies within the Data Protection Act 1998 or the information is required to be provided under the terms of the Freedom of Information Act 2000 or any subsidiary regulation.

6.3 Additional statutory restrictions apply to the disclosure of certain information for example Criminal Records, HIV and AIDS, Assisted Conception and Abortion, Child Protection etc. Information about these will be included in the relevant Information Exchange Agreement.

6.4 Where the provision of anonymised or pseudonymised data is adequate, practitioners must use these as a preferred method.

6.5 The partner organisations will ensure that information is requested and shared on the principle that it will be made available only on a justifiable "need to know basis". This means that staff will have access to information only if the function they are required to fulfil in relation to a particular service user cannot be achieved without access to the information in question. It may not be necessary to disclose all information held regarding a service user and only such information as is relevant for the purpose for which it is disclosed should be passed under the sharing arrangement to the recipient(s).

6.6 **Requests by carer's or other family members for service user information**

This protocol is an agreement between professionals within and across partner agencies. Requests from carers or other family members fall outside of this agreement and should be dealt with through each organisations local policies and procedures.

6.7 It must however be noted that the principles of confidentiality and data protection must always be applied within this context and that there is not an automatic right for carers or others to have access to information about any vulnerable person (even a family member) without the consultation, agreement and informed consent of the person in question.

7. Principles underpinning this

The partner organisations agree:

- to share information with each other where it is lawful and when they are required to do so;
- to comply with the requirements of the Data Protection Act 1998 and in particular with the 8 Data Protection Principles. (for more information on the 8 principles, see **Appendix 1**)
- to inform individuals when and how information is recorded about them and how their information may be used;
- to ensure that adequate technical and non-technical security measures are applied to the personal data they hold and transfer;
- to develop local Information Sharing Agreements that govern the way transactions are undertaken between partner organisations and with other organisations that are not party to this protocol;
- to promote staff awareness of the protocol;
- to promote public awareness of the need for information sharing through the use of appropriate communications media.

8. Sharing with consent

8.1 Choice, control and empowerment for service users are core principles throughout all areas of service delivery. These principles should also be considered as key elements in terms of the information partners gather, retain and share within the terms of this agreement. As such:

8.2 Partner organisations will seek informed explicit consent from the individual concerned before sharing his / her personal information in accordance with this protocol, unless there is a specific reason for this not being possible or where doing this would undermine the purpose of sharing that information.

8.3 In seeking consent to disclose personal information, the individual concerned will be made fully aware of the nature of the information, that it may be necessary to share, who the information may be shared with, the purposes for which the information will be used and any other relevant details including their right to access, withhold or withdraw consent.

8.4 All partner agencies will ensure that the details, including any conditions, surrounding consent (or refused consent) are clearly recorded on the individual's manual and / or electronic record in accordance with their agency's policies and procedures.

8.5 For further guidance on consent, please see **Appendix 2.**

9. Sharing without consent

9.1 There are circumstances when it is lawful to disclose personal information about an individual without their consent.

9.2 The Data Protection Act 1998 recognises that in certain circumstances the public interest requires the disclosure of personal information and creates certain exemptions from the non-disclosure provisions. These exemption disclosures include:

- disclosures required by law or in connection with legal proceedings
- disclosures required for the prevention or detection of crime
- disclosures required to protect the vital interests of the individual concerned
- where there is an overriding public interest.

9.3 The decision to disclose under these circumstances must be documented and include the reason for the decision, who made the decision, who the information was disclosed to and the date. A decision not to share information must also be recorded.

9.4 Where data needs to be shared in order to fulfil statutory requirements, these requests will be considered and approved by the appropriate Caldicott Guardian, Data Protection Officer, Information Risk Officer, Freedom of Information Officer or those with similar responsibilities from the partner organisations.

9.5 If you are unsure about whether it is lawful to disclose information without consent, seek legal advice or contact your organisation's Data Protection Officer or other designated officer as above.

9.6 For further guidance on consent, please see **Appendix 2.**

10. Organisational responsibilities

10.1 A number of safeguards are necessary in order to ensure a balance between maintaining confidentiality and sharing information appropriately. Organisations who share information under this protocol will adhere to the following:

10.2 Ensure staff are aware of and comply with:

- their responsibilities and obligations with regard to the confidentiality of personal information about people who are in contact with their agency
- the commitment of the organisation to share information legally and within the terms of an agreed specific information sharing agreement
- the commitment that information will only be shared on a need-to-know basis
- the understanding that disclosure of personal information which cannot be justified, whether intentionally or unintentionally will be subject to disciplinary action, and maybe subject to legal sanctions

10.3 Ensure information disclosed is recorded appropriately by:

- ensuring that all personal information that has been disclosed to them under an agreement is recorded accurately on that individual's manual or electronic record in accordance with the agency's policies and procedures
- putting in place procedures to record the details of the information shared, the provider and who received the information

10.4 Those organisations party to this protocol will put in place documented policies and procedures governing:

- the secure storage of all personal information retained within their manual and / or electronic systems
- the secure transfer of personal information both internally and externally

10.5 Such procedures must cover:

- Internal and external postal arrangements
- Verbal communications (phone, meetings etc)
- Facsimiles
- Electronic mail
- the access by their employees and others to personal information held in manual or electronic systems, and to ensure that access to such information is controlled and restricted to those who have a legitimate need to have access
- the retention and disposal of records containing personal information.

10.6 Data quality - Information shared should be of a good quality and it is recommended that the information shared follows either the Audit Commissions six principles of data quality, or other appropriate guidance used by the organisations sharing the information. The six data quality principles are:

- Accuracy;
- Validity;
- Reliability;
- Timeliness;
- Relevance and;
- Completeness

10.7 Further information about these principles can be found in the Audit Commission document entitled Improving information to support decision making: standards for better quality of data through the following link

10.8 **Data Security** – All Partners must have systems and processes in place to ensure that any information that is gathered, retained or shared complies with **Principle 7 of the Data Protection Act (appendix 1)** and is protected by appropriate security.

10.9 http://www.audit-commission.gov.uk/aboutus/howwearerun/ourstrategy/strategicobjectives/dataquality/pages/improvinginformation.aspx#downloads

11. Access to information

11.1 In line with the core principles of service user choice, control and empowerment, partner organisations will:

11.2 Maintain accurate, up-to-date and relevant records and will fully inform individuals about the information that is recorded about them, who may see their information, for what purposes and their right to access or object to having their personal information disclosed.

11.3 Under the Data Protection Act 1998, individuals also have the right to access, (subject to exemptions), information held about them and to correct any factual errors that may have been made. Where records are rectified, whether at the request of the individual or otherwise, any changes made as a result will be recorded and communicated to all organisations with whom the data had previously been shared.

11.4 Requests for access to information, objection or amendment should be sent to the relevant organisation's data controller.

12. Sharing with organisations who are not signatories to this protocol

12.1 Any organisation who is not party to this overarching protocol, but who wishes to share information may do so, providing that there is an existing Information Sharing Agreement in place with the third party, that they agree to comply with the terms of this overarching protocol and have adequate technical and non-

technical security arrangements in place.

13. Monitoring and Review

13.1 The LSAB will, in conjunction with partner organisations, review this overarching protocol annually unless new or revised legislation necessitates an earlier review.

13.2 Each partner organisation will be individually responsible for monitoring and reviewing the implementation of the protocol and any individual Information Sharing Agreements they may have.

14. Breach of Confidentiality

14.1 All agencies who are party to this protocol will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal information whether intentional or unintentional.

14.2 In the event that personal information shared under this protocol is or may have been compromised, whether accidental or intentional, the organisation making the discovery will, without delay:

- inform the organisation who provided the data of the details;
- take steps to investigate the cause;
- take disciplinary action against the person(s) responsible, if appropriate;
- take appropriate steps to avoid a repetition;
- take appropriate steps, where possible, to mitigate any impacts.

14.3 On being notified of a breach, the original information provider along with the organisation responsible for the breach, and others as appropriate, will assess the potential implications for the individual whose information has been compromised, and if necessary will:

- Notify the individual(s) concerned;
- Advise the individual(s) of their rights; and
- Provide the individual(s) with appropriate support.

14.4 Where a breach is identified as serious, it may have to be reported to the Information Commissioners Office. The original information provider, along with the breaching organisation and others as appropriate, will assess the potential implications, identify and agree appropriate action.

15. Complaints

15.1 Partner organisations must have in place procedures to address complaints relating to the disclosure of information. The partner organisations agree to co-operate in any complaint investigation where they have information that is relevant to the investigation. Partners must also ensure that their complaints procedures are well publicised.

15.2 If the complaint affects more than one partner organisation it should be brought

to the attention of the appropriate complaints officers who should liaise to investigate the complaint.

16. Organisational and individual responsibilities

16.1 Disclosure of personal information without consent must be justifiable on statutory grounds, or meet the criterion for claiming an exemption under the Data Protection Act 1998.

16.2 Without such justification, both the organisation and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act 2000.

16.3 A full list of the exemptions can be found at the website of the Information Commissioners Office: http://www.ico.gov.uk/what_we_cover.aspx

16.4 Each partner will keep each of the other partners fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner of any data obtained in connection with this agreement.

17. Other possible areas of influence or consideration – current consultations

17.1 While it must be noted that these documents are currently at consultation stage, if they should be adopted (in full or in part) they may have impact on this agreement. Future development in terms of these documents will be reviewed in line with the review arrangements for this protocol.

17.2 **Current Consultation Documents**

"An Information Revolution: a consultation on proposals"
"Liberating the NHS: Greater choice and control"

Other documents for consideration;

"Social Care Record Guarantee for England"

Appendix 1 - The 8 Data Protection Principles

The Data Protection Act 1998 governs the protection and use of personal data. It sets out standards which must be satisfied when obtaining, recording, holding, using or disposing of personal data. These are summarised by the 8 Data Protection Principles below. Under the key principles of the Act, personal data must be:

Principle 1 - Processed fairly and lawfully

There should be no surprises – data subjects should be informed about why information about them is being collected, what it will be used for and who it may be shared with.

Principle 2 - Obtained and processed for specified purposes

Only use personal information for the purpose(s) for which it was obtained and ensure it is not processed in any other manner that would be incompatible with that purpose(s).

Principle 3 - Adequate, relevant and not excessive

Only collect and keep the information you require. It is not acceptable to collect information that you do not need. Do not collect information 'just in case it might be useful one day'

Principle 4 - Accurate and kept up to date

Have in place mechanisms for ensuring that information is accurate and up to date. Take care when inputting to ensure accuracy and have local procedures in place to manage requests for information to be amended.

Principle 5 - Not kept for longer than is necessary

The legislation within the area you are working in, will often state how long documents should be kept. Information should be disposed of in accordance to your organisation's disposal policy.

Principle 6 - Processed in accordance with the rights of the data subject under the Act.

These rights include the right to:

- Make subject access requests
- Prevent the processing of data which is likely to cause them substantial damage or substantial distress
- Prevent processing for the purposes of direct marketing
- Be informed about automated decision making processes that affect them
- Prevent significant decisions that affect them from being made solely by automated processes
- Seek compensation if they suffer damage or distress through contravention of the Act

- Take action to require the rectification, blocking, erasure or destruction of inaccurate data
- Request an assessment by the Information Commissioner of the legality of any processing that is occurring

Principle 7 - Protected by appropriate security

This can be broken down into two elements:

Practical - this involves:

- ensuring the confidentiality of faxes by using Safe Haven /secure faxes,
- keeping confidential papers locked away,
- ensuring confidential conversations cannot be overheard
- ensuring information is transported securely

Organisational - all organisations should have:

- good information management practices
- guidelines on IT security
- procedures for access to personal data
- a retention and disposal policy for confidential data

Principle 8 - Not transferred to a country or territory outside the EEA without an adequate protection

If sending information outside the EEA, ensure consent is obtained and it is adequately protected. Consider carefully what is posted on websites or sent via email. Where appropriate, obtain approval from the data controller.

Appendix 2 - Consent: Guidance notes

Consent

In line with the core principles of choice, control and empowerment, service users must be consulted and where possible give their informed consent before their information is shared outside of the existing agreements in place by those who hold their information.

For consent to be valid, it must be:

- fully informed - the individual is aware of what information will be shared, with whom and for what purpose, and who controls the data (data controller);
- specific - a general consent to share information with 'partner organisations' would not be valid. Specific means that individuals are aware of what particular information we will share, who with and for what purpose;
- a positive indication by the data subject - the provision of opt outs on forms would therefore not obtain the consent of an individual. Refer to your organisation's Information Governance team for guidance on opt-out policy;
- freely given – the individual is not acting under duress from any party.

Individual organisations may have their own procedures for dealing with issues of implicit / explicit consent in order to allow it to meet its lawful obligations. Please refer to your organisation's procedures.

The person giving the consent must also have the capacity to understand what they are consenting to.

To give valid informed consent, the person needs to understand why their information needs to be shared, what type of information may be involved, who that information may be shared with and the possible consequences if it is not shared (if relevant).

The person should also be advised of their rights with regard to their information namely:

- the right to withhold their consent
- the right to place restrictions on the use of their information
- the right to withdraw their consent at any time
- the right to have access to their records

In general, once a person has given consent, that consent may remain valid for an indefinite duration unless the person subsequently withdraws that consent. However, it is best practice for practitioners to review this at every contact.

If a person makes a voluntary and informed decision to refuse consent for their personal information to be shared, this decision must be respected unless there are sound legal grounds for disclosing without consent. The consequences of not providing consent should be explained, e.g. such as not receiving the right service / amount of support.

New consent will be required where there are to be significant changes to:

- the personal data that will be shared,
- the purposes for which it will be shared, or
- the partners involved in the sharing (i.e. the proposed data sharing is not covered by the original fair processing notice).

Capacity to consent

The Mental Capacity Act (MCA) 2005 makes an automatic presumption of an individual's capacity to make decision for themselves unless (through an impairment of the brain) it can be shown that they are unable to do so.

In terms of assessing capacity, the MCA sets out a 4 stage functional test of capacity, namely that the individual is able;

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

Young Persons

Section 8 of the Family Law Reform Act entitles young people aged 16 or 17, having capacity, to give informed consent.

The courts have held that young people (below the age of 16) who have sufficient understanding and intelligence to enable them to understand fully what is involved will also have capacity to consent. This is augmented by the Gillick Competency.

It should be seen as good practice to involve the parent(s) or guardian / representative of the young person in the consent process, unless this is against the wishes of the young person.

In the case where the wishes of a young person, who is deemed competent to give consent, are opposed to those of their parent / carer, then the young person's wishes should take precedent.

Recording consent

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

The consent form should indicate the following:

- details of the agency and person obtaining consent;
- details to identify the person whose personal details may / will be shared;
- the purpose of sharing personal information;

- the organisation(s) with whom the personal information may / will be shared;
- the type of personal information that will be shared;
- details of any sensitive information that will be shared;
- any time limit on the use of the consent;
- any limits on disclosure of personal information, as specified by the individual;
- details of the person (guardian/representative) giving consent if appropriate.

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

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

Disclosure without consent

Disclosure of personal information without consent must be justifiable on statutory grounds, or meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act 2000

There are exceptional circumstances in which a service user's right may be overridden, for example:

- if an individual is believed to be at serious risk of harm, or
- if there is evidence of serious public harm or risk of harm to others, or
- if there is evidence of a serious health risk to an individual, or
- if the non-disclosure would significantly prejudice the prevention, detection or
- prosecution of a crime, or
- if instructed to do so by a court.

In deciding whether or not disclosure of information given in confidence is justified it is necessary to weigh the harm that would result from a breach of confidence against the harm that might result if you fail to disclose the information.

Legislation which permits the sharing of data without consent includes:

- NHS (Venereal Diseases) Regulations 1974
- Notifications of Births and Deaths Regulations 1982
- Codes of Practice, Mental Health Act 1983, s 1.3 – 1.13 and s 14
- Police and Criminal Evidence Act 1984
- Public Health Act 1984 and Public Health (Infectious Diseases) Regulations 1998
- Children's Act 1989 s 47
- Abortion Regulations 1991
- Finance Act 1994
- VAT Act 1994, s 91
- Criminal Procedure Investigation Act 1996

- Social Security Administration (Fraud) Act 1997
- Audit Commission Act 1998
- Crime and Disorder Act 1998, s 115
- Data Protection Act 1998, schedule 2 and schedule 3
- Terrorism Act 2000 s 19
- Civil Contingencies Act 2004

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

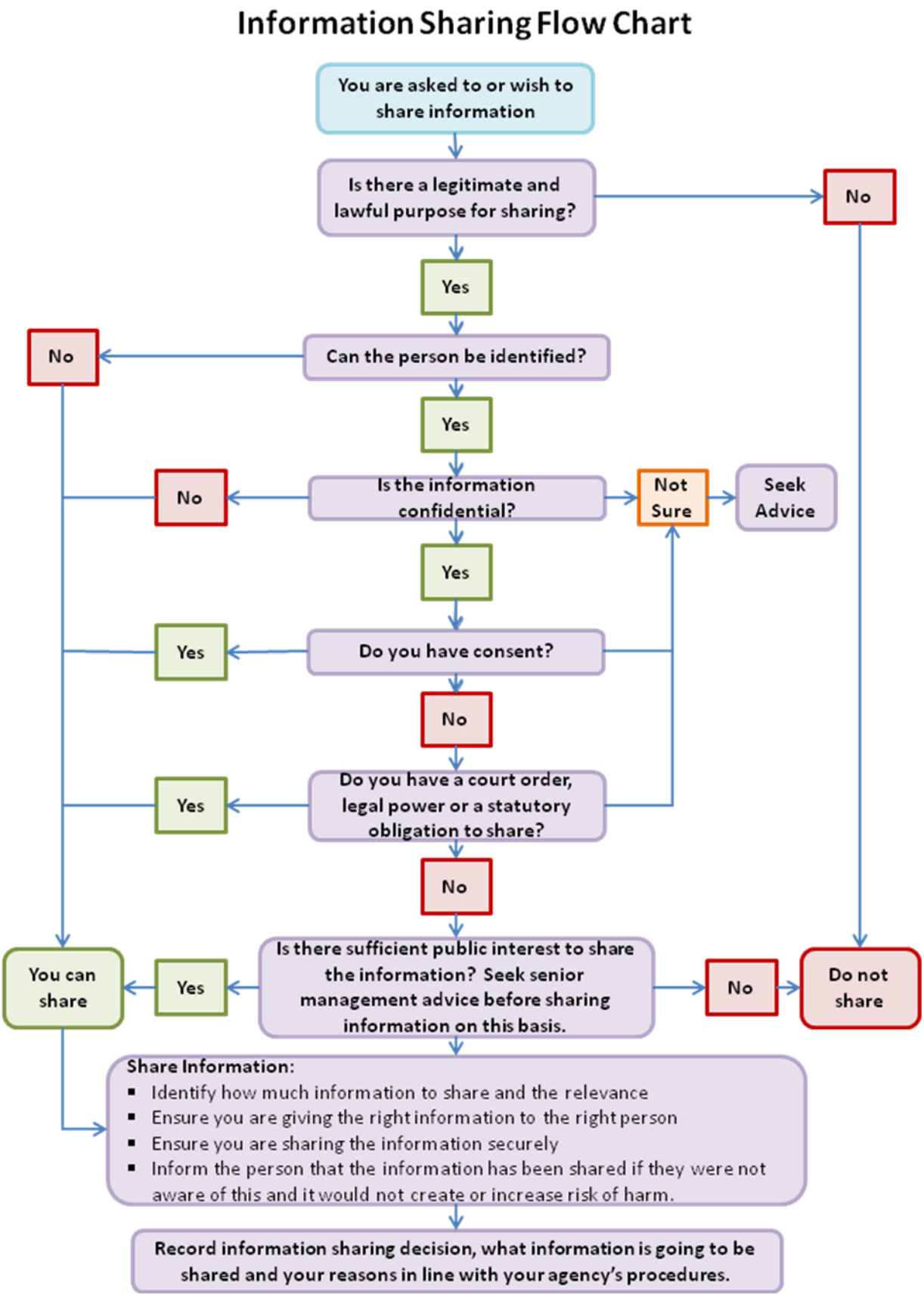
If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed.

A record of the disclosure will be made in the service user's paper or electronic file record and the service user must be informed if they have the capacity to understand, or if they do not have the capacity, then any person acting on their behalf must be informed.

If information is disclosed without consent, there may be some exceptional circumstances (particularly in the context of police investigations or child protection work) where it may not be appropriate to inform the service user of the disclosure of information. This situation could arise where the safety of a vulnerable adult (or child) would be jeopardized by informing the service user of such a disclosure.

In many such situations it will not be a case of never informing the service user, but rather delaying informing them until further enquiries have been made. Any decision not to inform, or to delay informing, should be recorded on the service user's paper or electronic file record, clearly stating the reasons for the decision, and the person making that decision.

Appendix 3 - Information Sharing Flowchart



Appendix 4 - Record of Disclosure Form

Confidential Record of Disclosure	
Service user name	
Service user D.O.B	
Local record identifier	
NHS number (if relevant)	
Description of data disclosed	
Reason for disclosure	
Recipient(s) of the data	
If disclosure is made without consent, please state reasons	
Reasons for refusal / limited disclosure (if appropriate)	
Disclosing organisation	
Disclosed by	
Authorised by	
Date of disclosure	

A copy of this disclosure record should be retained on the service user's file.

Appendix 5 - Seven Golden Rules for Staff on Information Sharing

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 (and/or their family where appropriate) 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

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

Harrow COUNCIL
LONDON

& our Partners

Committed to Safeguarding Adults

Harrow COUNCIL
LONDON

in partnership with:

AGE Concern HARROW
HAD Harrow Association of Disabled People
mind For better mental health
Harrow MENCAP Providing opportunity, promoting change
METROPOLITAN POLICE Working together for a safer London
Royal National Orthopaedic Hospital NHS Trust
The North West London Hospitals NHS Trust
Central and North West London NHS Foundation Trust
NHS Harrow
HAVS
LinkUp
Princess Royal Trust Carers Support Harrow
support for living
FREMANTLE Passionate about Care

Harrow COUNCIL LONDON & our Partners, Committed to Safeguarding Adults

Adult abuse - break the silence

REPORT IT

If you or someone you know is being abused, hurt or exploited, please call Harrow Council's Safeguarding Adults Service

Abuse can be physical, sexual, financial, psychological, discriminatory or neglect.

Safeguarding Adults Service

during office hours:

tel: **020 8420 9453**

at all other times

020 8424 0999

fax: 020 8416 8269

email: safeguarding.adults@harrow.gov.uk

web: www.harrow.gov.uk/safeguardingadults