Leeds Safeguarding Adults Partnership

INFORMATION SHARING AGREEMENT
July 2013

(Annex 12 of the Board MEMORANDUM OF UNDERSTANDING)

Safeguarding the right of vulnerable adults to live free from abuse & neglect

"Leeds - A *Safe* Place for Everyone"

Version 1
October 2010 – Appendix A, Access Agreements added 21 February 2013
Version 2
July 2013 – removal of references to Leeds Interagency Protocol for Sharing Information (2008)

Leeds Safeguarding Adults Partnership Information Sharing Agreement (ISA) July 2013

This agreement is written to promote the sharing of **personal data and / or sensitive** personal data, as defined by the Data Protection Act (1998) in the specific context of Adult Safeguarding. It describes:

a) the information which will be shared between the partner organisations listed, and
b) the arrangements for assisting compliance with relevant legislation and guidance, including the Data Protection Act (1998).

The following statement should guide all information sharing within the Partnership:

Whenever there is a need to share personal data and / or sensitive personal data to protect an adult at risk of harm, the specific reasons for sharing the information should be recorded, along with why it is considered relevant. The volume and detail of information shared must always be sufficient but not excessive for the required purpose. Wherever possible, decisions to share information should be made within the context of appropriate support, rather than by staff acting alone.

Where information is fully anonymised, or is otherwise non-identifiable or wholly statistical in nature it is not necessary to apply this agreement. Care must be taken however to establish that information is fully anonymised, as the obvious fields of person-identifiable data may not be the only positive identifiers within shared material.

Background

Leeds Safeguarding Adults Partnership recognize the need to provide clear guidance to staff in partner organisations on when and how to share information, in order to both:

a) establish the truth about allegations of abuse or neglect of vulnerable adults, and
b) prevent abuse or neglect of vulnerable adults.

Information sharing agreements do not in themselves make the sharing of personal data and sensitive personal data legal or ethical. The Data Protection Act (1998) sets out the context in which information may be used legally.

More detailed guidance will be developed, in line with this agreement, if required.

1. Parties to the Agreement:

Partner Organisations
Leeds City Council Adult Social Care
NHS Leeds Clinical Commissioning Groups
Leeds Teaching Hospitals Trust
Leeds Community Healthcare Trust
Leeds and York Partnership NHS Foundation Trust
West Yorkshire Police
West Yorkshire Probation Service
Leeds City Council Environment and Neighbourhoods Housing Services
Leeds City Council Community Safety
West Yorkshire Fire Service
Leeds City Council Children's Services
Leeds ALMOs
Leeds City Council Legal Services

2. Information Sharing Purposes:

1. To seek advice about a specific adult safeguarding situation or to establish grounds for an adult safeguarding investigation.
2. To prevent or detect a crime, or support the prosecution of offenders.
3. To make an adult safeguarding referral.
4. To protect a vulnerable adult.
5. To make a referral to a partner organisation for immediate action to protect an adult.
6. To establish the potential need for involvement of partner organisations in adult safeguarding work (investigation, prosecution or protection arrangements).
7. To plan an adult safeguarding investigation.
8. To initiate and conduct an adult safeguarding investigation.

9. To make a referral to organisations for the purposes of requesting or amending services to persons at risk of abuse.

10. To make a referral to organisations for the purposes of requesting or amending services to those suspected of perpetrating abuse.

11. To make a referral to the Independent Safeguarding Authority (ISA) Vetting and Barring scheme or to provide information to the ISA for the purposes of them coming to a barring decision.

12. To notify the Care Quality Commission who may need to take action relating to an alleged perpetrator that is a registered care provider.

13. To notify the Charity Commission who may need to take action relating to an alleged perpetrator that is a registered charity.

14. To notify employers who may need to take action against perpetrators who are paid or unpaid staff or volunteers and are thought to pose a risk in respect of the nature of their work.

15. To notify service providers of a risk posed by a service user.

16. To inform the development of multi-agency policies and strategies for protecting adults at risk of abuse.

17. To monitor and review adult safeguarding referrals and the impact of adult safeguarding policies and procedures, including both the equalities (race, ethnicity, gender, sexuality, age, disadvantage and disability) impact of the policies and the outcomes for individuals. This may include both quantitative and qualitative information, personal data and sensitive personal data, the personal views of individuals and expressions of relevant professional opinion.

18. To conduct adult safeguarding serious case reviews.

19. To deal with complaints, grievances and professional and administrative malpractice.

3. Information to be Shared:

What types of information will be shared?

There are two distinct classifications of data covered by the Data Protection Act (1998): Personal data and sensitive personal data.

Personal data includes data relating to a living individual who can be positively identified from the data, or from the data and other information which is at the disposal of other individuals or is in the public domain. Personal data includes obvious identifiers such as names, addresses, dates of birth, as well as NHS or National Insurance numbers. Facial photographs and CCTV footage are also regarded as personal data, as are descriptions or photographic records of unique scars, tattoos or other markings.

Sensitive personal data includes data relating to racial or ethnic origins, religious beliefs or similar belief systems, political opinions and affiliations, trade union membership, physical or mental health (including disabilities), sexual life, the commission or alleged commission of offences, and criminal proceedings.

Information relating to adult safeguarding may involve a wide range of both personal data and sensitive personal data, in circumstances relating to up to seven types of abuse:

- Discriminatory
- Emotional / Psychological
- Financial
- Institutional
- Neglect
- Physical
- Sexual

It is impossible to cover all potential scenarios in this agreement. The guidance is therefore to:

1. Share as much as, but no more than, is necessary.
2. Always document the reasons for sharing personal data and sensitive personal data.
3. Record why it is believed the data shared is relevant and proportionate.

4. Methods Used for Sharing:

Within the Safeguarding Process, information may be transferred in the following ways:

- Verbally, face to face, in wider meetings or on the telephone.
- In written communications, (for example, alert / referral forms, letters, statements or reports) transferred in hard copy through internal or external mail services.
- In written communications transferred by fax.
- Documents transferred on CD, DVD or other electronic digital media.
- In written information transferred by email
- Information accessed in situ, via provision of access to organisational databases or records.

When each of these methods is used it is essential to consider the safest way to record and mark the information, and to assure safe transit and delivery. Information should be appropriately secured in transit, transferred by methods aligned to the best practice specified in the "Data Handling Procedures in Government Report – June 2008".

1. Verbal conversations and interviews should be recorded in a statement that is agreed by the information giver. Care must be taken to record and denote information clearly as fact, statement or opinion and to attribute any statement or opinion to the owner. All information should be recorded in such a way that it can be used as evidence in court, should that be required at a later date.

2. Meetings should be recorded in minutes that are agreed by the delegates present.

3. Written communications containing confidential information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation. They should be clearly marked "Private & Confidential – to be opened by the recipient only".

4. When files are transferred on CD, DVD or other electronic digital media, the files should be encrypted to an appropriate standard, with decryption keys / passwords supplied separately.

5. When confidential information is sent by email, it should be sent and received using secure government domain email addresses, to ensure encryption of information in transit. Secure emails include the following email address domains:
   - GSi (*.gsi.gov.uk);
   - CJX (*.police.uk or .pnn.police.uk);
   - GSE (*.gse.gov.uk);

- GSX (*.gsx.gov.uk);
- GCSX (*.gcsx.gov.uk);
- SCN (*scn.gov.uk);
- CJSM (*cjsm.net);
- MoD (*.mod.uk);
- NHS (*.nhs.net).

In-transit security is reliant on BOTH the sender AND recipient using one of the email domains listed above. In the absence of this, the SENDER will need to encrypt the content of the email using additional software. This may be achieved by sending an encrypted attachment.

6. When confidential information is sent by fax, it should be sent to a "safe haven" fax. This is a fax machine that is managed in such a way that you can be confident that information can be transferred to it in the knowledge that safeguards are in place to ensure its security and that access is restricted to assure confidentiality.

7. In all transfer scenarios, the onus is on the SENDER to ensure that:

   - Information is transferred securely
   - The chosen method is acceptable to and workable by the recipient
   - Information has reached the required recipient

8. In the event that a recipient receives information by an unsecured route, it is incumbent on the recipient to advise the sender and agree a secure route for future transfers of information.

5. Need to Know

Key roles of individuals within the Safeguarding process will govern whether they need to know information about alleged victims, alleged perpetrators, witnesses and other information pertaining to incidents.

In addition to alerters, referrers, investigators and safeguarding coordinators, other people who may contribute and receive information include other staff and managers, volunteers, family members, carers and witnesses. These people may be invited to contribute to strategy discussions or meetings, investigations and case conferences and reviews.

At all times it is essential to be certain of the reasons why an individual or a meeting needs access to the information. Is it necessary for this individual or meeting to know this information in order to conduct the investigation or to protect an alleged victim?

Where an investigation involves more than one alleged victim, it may be necessary to partition meetings so that contributors can be invited only for specific items, based on their need to know.

6. Supporting Documentation:

West Yorkshire Safeguarding Adult Policy and Procedure 2013
(available on www.leedssafeguardingadults.org.uk)

Leeds Mental Capacity Act Policy and Procedure, and Mental Capacity Assessment and Best Interest Decision Recording Tools
(available on www.leedssafeguardingadults.org.uk)

ICO Data Sharing Code of Practice
(available at
http://www.ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

Data Handling Procedures in Government: Final Report – June 2008
(available at:
https://www.gov.uk/government/publications/data-handling-procedures-in-government

Safeguarding Partnership Support Team Advice line (phone 0113 224 3511)

Advice available from each organisation's Data Protection specialist or Caldicott Guardian.

7. Information Retention and Disposal:

The Data Protection Act (1998) requires that personal data and sensitive personal data is not retained for longer than necessary. Partner organisations may have their own organisational, legal or procedural requirements for records retention and disposal. These retention schedules should be observed and applied at all times.

Where no such organisational procedure exists, it is essential to keep pertinent information as long as there continues to be a need for protection arrangements, to ensure that protection arrangements are not compromised and equally that such information is securely disposed of when no longer required.

8. Staff Development Issues:

Training and Workforce Development needs relating to information sharing in the Safeguarding process form part of the four-level training framework, based on key roles within the safeguarding process, and the competencies required:

Level 1: Alerter
Level 2: Referrer
Level 3: Investigator
Level 4: Safeguarding Coordinator and other specialist roles

As part of each partner's contribution to the Training and Workforce Development sub-group of the Safeguarding Adults Board, the needs of its workforce are considered against these four levels, and fed into training requirements for both the individual partner organisation and the partnership as a whole.

9. Consent from Individuals to Share their Personal Information:

Staff and volunteers should always seek consent from individuals before sharing their personal data and / or sensitive personal data, whenever possible and appropriate. They should record the consent, when given, on their organisation's standard consent documentation. Where it is not possible to obtain consent, this could be because:

- the individual does not have the mental capacity to consent
- it may not be safe to seek consent
- it may not be possible to seek consent for some other reason

In cases where it has not been possible to seek or obtain consent, staff or volunteers should always record the justification for sharing the information, and how this decision was arrived at.

1. If the individual does not have the mental capacity to consent, staff or volunteers should record this using their agency's Mental Capacity Assessment recording tool, and record their decisions to share information using their agency's Best Interests Decision recording tool.

2. If the subject has not given consent for reasons other than those covered by the Mental Capacity Act, one of the reasons from Schedule 2 of the Data Protection Act (1998) is required to justify the sharing of personal data, whilst a reason from Schedule 2 AND Schedule 3 is required to share sensitive personal data. Those reasons with particular relevance to this agreement are included below:

Schedule 2 – Justifications for the sharing of personal data:

- Compliance with the legal obligations of partner organisations
- Protecting the vital interests of the subject
- Carrying out tasks or duties substantially in the wider public interest
- Pursuing the legitimate interests of the partner organisation

Schedule 3 – Justifications for the sharing of sensitive personal data:

- Compliance with employment law obligations
- Protecting the vital interests of the subject
- Legal advice and establishing or defending legal rights
- Public functions (including the administration of justice)
- Medical purposes and the provision of healthcare
- Detection of unlawful activity
- Protection of the public
- Confidential counselling
- Police processing

For further advice on justifiable grounds for sharing information, contact your organisation's Data Protection specialist or Caldicott Guardian.

10. Organisational Data Protection Contacts

Contact details for staff who can provide advice / support in relation to this Information Sharing Agreement:

Organisation	Lead Officer	Contact details
Leeds City Council Adult Social Care	Louise Whitworth	Louise.Whitworth@leeds.gov.uk
Leeds Community Healthcare Trust	Richard Birmingham	Richard.Birmingham@nhs.net
Leeds Teaching Hospitals NHS Trust	Johnny Chagger	Johnny.Chagger@leedsth.nhs.uk
West Yorkshire Police	Helen Crosland	Helen.Crosland@westyorkshire.pnn.police.uk
Community Safety	Inspector Steve Lavelle	stephen.lavelle@westyorkshire.pnn.police.uk
Leeds & York Partnership NHS Foundation Trust	Carl Starbuck	carl.starbuck@nhs.net
West Yorkshire Fire Service	Allan Darby	Allan.darby@westyorksfire.gov.uk
West Yorkshire Probation Service	Imogen Brown	Imogen.Brown@west-yorkshire.probation.gsi.gov.uk
Leeds City Council Environment and Neighbourhoods Housing Services	Debbie Forward	Debbie.forward@leeds.gov.uk
Leeds ALMOs	Jill Wildman	jill.wildman@enehl.org.uk
Head of Safeguarding Adults	Hilary Paxton	hilary.paxton@leeds.gov.uk

11. Access Agreements

Where information is to be shared via granting inter-organisational access to systems operated by partner organisations, the 'owning' organisation of the system will draft and agree an Access Agreement with the partner organisation to govern the activities of partner staff using the system.

A template for this purpose can be found in Appendix B of this document.

12. Discipline

Although this agreement seeks to promote the sharing of information between partner organisations, use of the information shared should never exceed the purposes or intentions of the original reason for sharing.

Where allegations are made that information has been used inappropriately, or that the confidentiality of subjects has been breached, partner organisations will co-operate in a full and frank investigation of these allegations.

In the event that any wilful misconduct is substantiated which resulted in a breach of subject confidentiality, this will be regarded as an act of serious or gross misconduct and acted upon accordingly.

13. Performance of this Agreement

Should any member of staff or volunteer working for a partner organisation feel that the letter and spirit of this agreement is not being honoured, or that barriers to legitimate sharing of information are being raised, this should be communicated to their organisation's representative on the Leeds Safeguarding Adults Partnership Board, who will in turn follow this up with their counterparts and Data Protection leads in the partnership organisation.

Approved by (Signatory Name): Dr Jim Isherwood – Medical Director & Caldicott Guardian

Signature: .....

For (Partner Organisation): Leeds and York Partnership NHS Foundation Trust

Date: 23rd July 2013

Once signed, this document should be sent to the Leeds Safeguarding Adults Partnership Support Team. Copies should be retained by the named person above and be made available for inspection. A copy should also be sent to the Data Protection Officer / Caldicott Guardian of each partner organisation, if this is a different person.

Appendix A

Further to **"11. Access Agreements"** in the information sharing agreement above, the Leeds Safeguarding Adults Board has recommended that the Leeds City Council (LCC) Adult Social Care (ASC) Case Management System (ESCR or its successor) should be used for recording and reporting Safeguarding Adults data across Health and Social Care. This has been agreed with the host partner organisation, Adult Social Care.

The Government expects and requires Adult Social Care to report nationally to the Health and Social Care Information Centre on all safeguarding activity. It is felt that the only way to ensure consistent, accurate and comprehensive recording of data is to create a single format in one system. Additionally the draft Care and Support Bill plans that Local Authorities will have new Safeguarding Intervention powers. Given these responsibilities, ASC's Case Management System is the system of choice.

In order to accomplish the task it has been agreed that a small number of named, designated safeguarding adults staff at Leeds Teaching Hospitals NHS Trust (LTHT) and Leeds and York Partnership NHS Foundation Trust (LYPFT) should be granted read / write access to ASC Case Management System.

The following provisions will be made:

- The recommended approach is to provide the nominated staff at LTHT and LYPFT with access to ASC Case Management System via the LCC network using an LCC device (single).
- A relevant senior manager from both LTHT and LYPFT will sign general Access Agreements to both the LCC network and ASC Case Management System.
- The individual staff requiring access to the system will sign the LCC confidentiality agreement.
- Access will be granted solely for the purpose of recording the agreed Safeguarding data and there will be no "legitimate relationship" to access the data of any other service user, or any other data of the vulnerable adult.
- A course has been developed to train the relevant staff from partner organisations in order to enable them to record Safeguarding data.
- ASC will ensure that we can isolate the set of health / mental health safeguarding adults referral and investigation data so we can remove them from other adult social care statutory returns. This can be easily achieved through the use of a referral outcome and owner team.

Appendix B

Agreement between Leeds City Council and Leeds and York Partnership NHS Foundation Trust for access to the LCC Case Management System and LCC Network

1. Background

This Agreement is between Leeds City Council Adult Social Care (LCC ASC) and Leeds and York Partnership NHS Foundation Trust (LYPFT). The Agreement is in respect of granting access for authorised employees of LYPFT to the LCC ASC Case Management System and LCC Network.

The purpose of the Agreement is to ensure that effective safeguards are in place for the secure and confidential use of the LCC ASC Case Management System by authorised staff of LYPFT.

Access to Leeds City Council network is via ***temporary login to Leeds City Council network*** which must be used exclusively to enhance the quality of service user care, or to facilitate administration in the Health & Social Care and the professional work of those providing care.
LYPFT are required to have arrangements in place to ensure that the requirements of this Agreement and their own organisational Information Security and Confidentiality Policies are adhered to.

2. Authorising access to Leeds City Council's network

Access can only be granted to an individual LYPFT member of staff where the following conditions are met:

- This Agreement has been signed by an authorised LYPFT signatory
- The employee has been authorised for access to Leeds City Council network by an appropriate Director of the relevant organisation and by the appropriate LYPFT Manager
- The employee has signed the declaration regarding compliance with Leeds City Council policies relating to security and confidentiality

3. Unacceptable use

Leeds City Council's network may NOT be used for any of the following:

1. The creation, downloading or transmission (other than for properly supervised and lawful purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
2. The creation, downloading or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
3. The creation, downloading or transmission of defamatory material
4. The transmission of material such that this infringes the copyright of another person
5. The transmission of unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks
6. Non-Healthcare profit-making activity that grossly abuses the service
7. Other activities that do not benefit service user care or that do not support the professional concerns of those providing that care, where those activities constitute gross abuse of the service
8. Gross abuse of the service by the unsolicited sending of inappropriate e-mail to large numbers of people, whether Leeds City Council network or on the Internet

9. Deliberate unauthorised access to facilities or services accessible via the Leeds City Council network
10. Deliberate activities with any of the following characteristics

- flagrant wasting of staff effort or networked resources, including time on end systems accessible via Leeds City Council network and the effort of staff involved in the support of those systems
- corrupting or destroying other users' data
- violating the privacy of other users
- disrupting the work of other users
- using Leeds City Council network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment)
- continuing to use an item of networking software or hardware after the Leeds City Council network has requested that use cease because it is causing disruption to the correct functioning of Leeds City Council network
- other misuse Leeds City Council network or networked resources, such as the introduction of computer viruses
- where Leeds City Council network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable

4. Compliance with Leeds City Council Security and Confidentiality Policies

LYPFT staff will be required to comply with Leeds City Council policies on security and confidentiality when using Leeds City Council network. Staff will receive training on information governance issues prior to being authorised to use the system.

5. Penalties for misuse

If a member of LYPFT staff is demonstrated to have made unacceptable use of Leeds City Council network and / or internet and intranet, access rights will be revoked.
LYPFT will be required to take appropriate disciplinary action in such cases in accordance with their disciplinary policies.
Any illegal activity must be dealt with as grounds for summary dismissal.

6. Declaration of compliance

The declaration must be signed by an appropriate, authorised LYPFT signatory.
This declaration will remain valid for a period of three years. After that time, a fresh declaration should be signed. If the person signing this declaration leaves his/her post a fresh declaration must be signed by the new incumbent.

The signatory has responsibility for ensuring that all members of LYPFT staff who are authorised to use Leeds City Council Network, are fully aware of the terms of this declaration.

Details of authorised Leeds and York Partnership NHS Foundation Trust signatory:

Name: **Dr Jim Isherwood**

Post: **Medical Director & Caldicott Guardian**

Address: **Trust HQ, 2150 Thorpe Park, Century Way, Colton, Leeds LS15 8ZB**

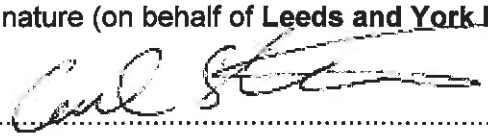
Telephone number: **0113 305 5000**

Email address: **jisherwood@nhs.net**

Declaration

I have read and understood the Agreement and will ensure that **Leeds and York Partnership NHS Foundation Trust Staff** will comply with its terms.

Signature (on behalf of **Leeds and York Partnership NHS Foundation Trust**)



.....

Print name: **Carl Starbuck – Information & Knowledge Manager**

Date: **22nd July 2013**

Authorisation by Leeds City Council:
This agreement has been authorised on behalf of the Council by:

Name .....

Signature .....

.....

Date .....