

Substance Misuse Services Information Sharing Agreement

February 2010



Disclaimer

The contents should not be used as expert opinion, legal or otherwise. Professional advice should be sought where appropriate. Any liability arising from action taken in relation to the contents of the Agreement is excluded.

This Agreement has been drawn up within the framework of the Leeds Inter-Agency Protocol for Sharing Information which is available at the following link:

<http://www.leedspct.nhs.uk/about/?pagepath=About%20Us/Information%20Sharing/Protocol>

Substance Misuse Services Information Sharing Agreement

Contents

Section 1 – Development and scope of the Agreement

- Section 1.1 - Background
- Section 1.2 - Introduction
- Section 1.3 - Framework for confidentiality and information sharing
- Section 1.4 - Parties to this agreement

Section 2 – Information to be shared and its purposes

- Section 2.1 - Types of information to be shared
- Section 2.2 - Purposes for sharing information
- Section 2.3 - Consent to share information

Section 3 – Accessing the information

- Section 3.1 - Methods of access
- Section 3.2 - Retention of records
- Section 3.3 - Subject access requests

Section 4 – Training and staff development

- Section 4.1 - Information governance and confidentiality training
- Section 4.2 - System specific training
- Section 4.3 - Training on this ISA

Section 5 – Dissemination, breaches & complaints relating to this ISA

- Section 5.1 - Dissemination of this ISA
- Section 5.2 - Reporting breaches
- Section 5.3 - Managing complaints

Section 6 – Advice and guidance

Appendices:

- Appendix 1** – Specialist advice and contact details
- Appendix 2** – Key principles
- Appendix 3** – Example information leaflet for service users and Carers
- Appendix 4** – Breach reporting form
- Appendix 5** – ISA formal approval form
- Appendix 6** – IT System Acceptable User Agreement

Section 1

Development and scope of the Agreement

1.1 Background

Legislation, guidance and Government policy all emphasise the importance of confidentiality and the protection of personal information. Strong emphasis is also however placed on the need to share information in order to provide effective, integrated services.

Health and social care organisations in Leeds recognised the need to provide clear guidance on this issue and responded by establishing an interagency steering group who developed the Leeds Interagency Protocol for Sharing Information.

The Protocol is an over-arching framework for sharing information between health, social care and other agencies in Leeds. The main agencies covered include:

- Leeds Teaching Hospitals Trust
- Leeds Partnership Foundation trust
- NHS Leeds
- Leeds City Council
- Education Leeds
- West Yorkshire Police
- Yorkshire Ambulance Service
- NHS Direct
- Leeds Voice
- Advocacy Network Leeds
- Leeds Carers

The protocol focuses on requirements for sharing personal information about service users and clarifies the legal background on information sharing by providing practical guidance and a template document for developing an Information Sharing Agreement.

1.2 Introduction

This Information Sharing Agreement (ISA) has been developed in accordance with the **Leeds Interagency Protocol for Sharing Information** and must be read in conjunction and with reference to it. Copies are available from the information governance leads within your organisation or via the following web link <http://www.leedspct.nhs.uk/about/?pagepath=About%20Us/Information%20Sharing/Protocol>

This ISA has been commissioned by Safer Leeds to assist the appropriate sharing of personal information about service users across substance misuse services in Leeds.

This ISA will be used to assist in ensuring that:

- Information is shared in a secure manner
- Information is shared only on a 'need to know' basis

- Information is divulged only with the service user's informed consent (unless it is justified to share this information without consent see section 4)
- It is clear which post holders are able to deal with requests for disclosure
- There are clear procedures and time limits to be followed with regard to information sharing
- Information will only be used for the reason(s) it has been obtained

1.3 Framework for confidentiality and information sharing

There is a large volume of legislation and regulations in place to safeguard the processing of personal information. The key legislation is the Data Protection Act however there are additional considerations such as Caldicott and further information and guidance can be found in the **Appendices** of the **Leeds Interagency Protocol for Sharing Information**

<http://www.leedspct.nhs.uk/about/?pagepath=About%20Us/Information%20Sharing/Protocol>.

1.4 Parties to this Agreement

The following organisations were requested to be parties to this Agreement.

Leeds Mental Health Trust	West Yorkshire Probation Service
Leeds City Council	West Yorkshire Police
Leeds Teaching Hospitals Trust	HM Prison Service
Youth Offending Team	NHS Leeds
All drug services commissioned by the Safer Leeds Partnership	

Section 2 Information to be shared and its purposes

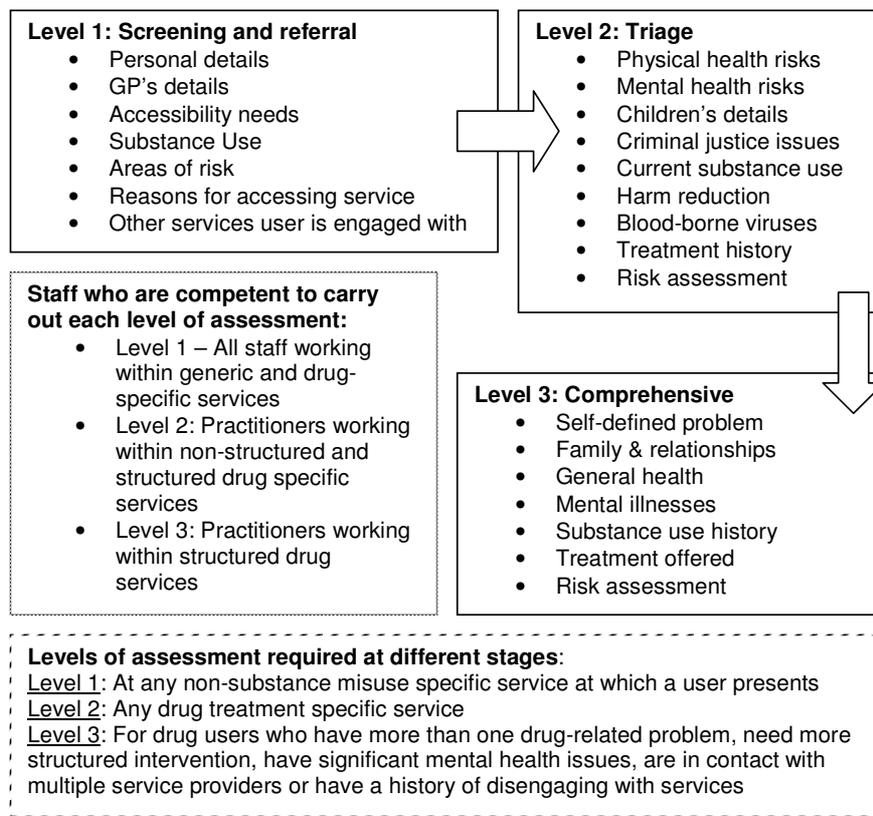
The Agreement covers the sharing of personal information about service users within and between the partner organisations listed in **Section 1.4**.

2.1 Types of information to be shared

The types of information that may need to be shared to ensure the most effective care for drug users are:

- Personal details (e.g. name, address, DoB, gender)
- Drug use
- Psychological, physical and legal problems
- Risk factors (e.g. self-harm, child protection issues, suicidal ideas, mental/physical health emergencies)
- Social issues

There are three levels of assessment, which is accompanied by a risk assessment, within the substance misuse field, and the types of information which are required at each stage are illustrated below:



2.2 Purposes for sharing information

Information may be shared under the Agreement for the following purposes:

- To facilitate the exchange of data, between organisations delivering within Safer Leeds Treatment and Recovery Service in order to:
 - Address issues around a service user's substance misuse
 - Facilitate lifestyle plans
 - Enable the provision of suitable treatment, accommodation and other support services
 - Minimise the risks associated with drug misuse
- To aid a co-ordinated approach to care planning for service users
- To ensure that information can be shared appropriately where this is justified by risk factors
- To facilitate sharing of anonymous information for the purposes of research and development on the prevalence of local drug use to aid the commissioning process

The Agreement has been approved only for the purposes listed above. If other information sharing purposes are subsequently identified these will be considered for inclusion by the Leeds Safer Leeds Governance Group.

2.3 Consent

Wherever appropriate, consent should be used as the basis for sharing information under this agreement.

Every adult has the right to make decisions and is assumed to have capacity to do so unless proven otherwise. (See **Section A** in the **Operational Procedures of the Leeds Interagency Information Sharing Protocol** for further details on the issue of consent)

Service users of each organisation should be given details on how their personal information will be used and what their rights are in relation to information disclosure.

The consent process should include the following steps:

- Seek consent at the assessment stage (or whenever a the need for onward referral to another agency is agreed with the service user).
- Provide a leaflet in an appropriate format for the service user with details of confidentiality, consent and information sharing issues (see appendix 3).
- Inform the service user that it will be necessary to collect and record personal information about them in order to provide appropriate services.
- Inform them that it may be necessary to share their information with other teams and organisations in order to provide these services. Let the service user know which teams and organisations this will include.
- Ask them for their consent for this to be done and indicate this on the appropriate consent fields (including NDTMS)
- Keep a record of whether consent is given or refused or whether any conditions are placed on the consent i.e. in terms of the types of information that can be shared or the organisations it can be shared with.
- If consent is refused explain the consequences of this i.e. that it may not be possible to provide them with some of the services they need
- If consent is refused, consider whether risks to the service user or others justify the sharing of information.
- Complete the Information sharing and consent form attached at appendix 4.
- Keep a record of any decision made

2.3 NDTMS reporting

NDTMS reporting is managed through the IT Case Management system. The key points to consider are:

- A client/patient's initials, date of birth, gender and part postcode are used for the national NDTMS. Although not fully identified data, these items of information still make it necessary to obtain explicit consent[†] from the client/patient before collecting data to send to the NDTMS.
- Ideally, this consent would be part of the process of obtaining consent in general, when explaining local data collection policies.
- The patient/client MUST be given the NDTMS information sheet (see help sheet 7), alongside the treatment service's confidentiality policy/leaflet, which explains what the information will be used for.

- If the client/patient refuses consent, record REFUSED in the patient record.
- If a treatment service has not previously provided data to the NDTMS but begins to do so for the first time, the service should seek retrospective consent from any existing clients. Where consent cannot be obtained, then mark the record as 'no consent'.
- Most clients/patients are reassured when they know why their data is collected and how it is shared. Become aware of the reasons for collecting various data items and how information is used within your service so that your clients/patients are fully enabled to make an informed decision.

[†] Explicit consent is usually given orally or in writing. It should be freely given in circumstances where the client has been appropriately informed. There should be an understanding of available options and any concerns and queries should have been addressed.

Section 3

Accessing the information

Staff should have access to information on a “need to know” basis i.e. only if the function they are required to fulfil at that particular point in time cannot be achieved without access to the information specified.

3.1 Methods of access

Transmission of paper documentation

Once an assessment has been carried out and an appropriate service has been identified to refer a service user to, the practitioner should telephone the service to discuss the referral with them. Once agreement has been reached verbally that the referral is appropriate, the screening and referral assessment along with the triage assessment (and comprehensive assessment where one has been completed) for continuation of treatment. Services should ensure a valid fax number is used within each partner organisation, checking these numbers regularly and ensuring the fax machines are located in a secure location where access is limited to dedicated personnel with a need to access the information. Faxes can then be sent securely with the patient identifiers. Faxes should always include a process a cover sheet and be marked as confidential and For the Attention Of a specific individual in the receiving service. These safeguards will prevent anyone other than the persons sending and receiving the information from accessing such sensitive data and will protect the service user's confidentiality

Screening and Referral Assessment

- Initially a telephone conversation will take place between the referring and receiving service to discuss the appropriateness of a referral. Care should be taken by both parties that personal details are not heard by other staff. These conversations should ideally take place in private locations and not publicly. If this is not possible then information should be transferred by more secure means. Once it has been agreed that the referral is appropriate, the information would be sent by fax to the receiving service

- A locally developed screening and referral form has been designed to capture key information by the referring service (service, worker's name, telephone no, address, referral date, appointment offered, actual appointment date) and some brief sensitive information. The receiving organisation should use their own recording mechanisms to record the details of incoming referrals to ensure that faxes do not go missing

Triage and Comprehensive Assessments

Ideally, the information given during a triage and comprehensive assessment should not be sent by fax but there will be times when this will need to happen due to the nature of the service, urgency etc. If sensitive data is to be sent via this method then two faxes should be sent – the first fax containing all information but not personal details, and the second fax containing personal details only. The second fax would only be sent when both parties are sure that the first fax has arrived safely. This would avoid the service user being identified if the first fax goes astray. The following precautions should also be taken:

- A safe haven fax should be used (one that is managed in such a way that its security is enhanced). These safeguards should include that:
 - The fax is sited in a secure room
 - The receiving organisation has a written policy for handling faxes which staff have been informed about and understand
 - Identified staff are responsible for collecting and delivering the faxed information to the appropriate person
- The referring organisation should telephone the receiving organisation to ensure that they are aware that a confidential fax is about to be sent and to confirm that an identified individual will collect and deliver it and that safe receipt will be confirmed
- The fax should be sent with a cover sheet stating that it is strictly confidential, for the practitioner who has discussed the referral only. In the event of error, the sender should be notified immediately
- The fax number should be double-checked before sending
- A log should be kept of confidential faxes sent, giving details of sender and receiver, date and time of transmission and a copy of the printout from the fax confirming transmission success

When information is being transferred by post:

- The information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation, marked "Personal and Confidential – to be opened by the recipient only".
- The designated person should be informed before the information is sent
- The information should not be opened at a central point and information should be restricted to those with a need to know
- The information should be limited to those details necessary in order for the designated person receiving the referral to carry out their role

In some situations it may be possible to actually hand deliver assessments to another service. Other methods of sharing information include email in appropriate circumstances. Services must ensure that electronic transfers of identifiable information

are adequately safeguarded (e.g. by the use of encrypted e-mails or via secure networks such as, pnn.police.uk/gsi.gov.uk/cjism.net/nhs.net)

As drug practitioners are engaged in multi-disciplinary teams and within different settings, confidentiality restrictions will be service specific. Confidentiality should be described in all service settings but issues will differ across services. For example:

- There will be specific confidentiality issues within prisons due to vital safety procedures and a duty to report breaches of security
- Substance misusers subject to a restriction on bail, drug rehabilitation requirement order (DRR), or any other community order that stipulates drug treatment is required, will need to give consent when they begin their order to probation staff
- Group situations will need to set confidentiality restrictions specifically for the group
- Open access services may need to strike a balance between confidentiality requirements and engagement. In order to make them accessible:
 - Anonymity may need to be maintained when service users are accessed through an outreach worker
 - It may also be appropriate to maintain anonymity when a service user accesses needle exchange, however information on confidentiality should be given out if possible
 - If service users do disclose information, confidentiality restrictions should be described so that if they do so in the future, this information will be disclosed with consent
- Drug practitioners may be asked to attend child protection conferences to give confidential information about a service user in relation to the safety of their child/children

Transmission and storage of information via IT Systems

Personal data will be held electronically in a central IT database. This system is commissioned by Safer Leeds as the agreed case management and prescribing tool. The IT System used will be an encrypted application at (a minimum) 128 bit encryption through SSL with a SHA1/AES algorithm. Certificates are used to provide authentication between the user and application. All data stored on the IT System and reports generated from the system must be used in accordance with the purposes indicated in section 2.2. All information stored on and/or accessed via the system will be used and managed in accordance with the principles outlined in this document.

Any other systems used within the partnership should be used and managed in accordance with the principles outlined in this document.

3.2 Retention of records

Records should not be kept longer than necessary and signatories to this ISA have agreed that records will be retained by the service provider for no longer than eight years after the conclusion of treatment. The following guidance clarifies record retention in 'other' circumstances:

- Children and young people's records should be kept until the service user's 25th birthday or 26th if the young person was 17 at the conclusion of treatment.
- The records of "mentally disordered persons" (as defined by the Mental Health Act 1983) should be kept for 20 years after no further treatment was considered necessary; or eight years after the service user's death, if they died while receiving treatment.
- Where legal action has been commenced, records should be kept as advised by legal representatives.

All records relating to a service user's care will be the responsibility of commissioned services until such point as the contract either comes to the contract end, is terminated by Safer Leeds Joint Commissioning Group or the organisation withdraws from providing the service. The documents will then be transferred to the newly commissioned provider taking over responsibility for delivery of that element of the Leeds Integrated Treatment System.

FOR FURTHER GUIDANCE CONTACT THE INFORMATION GOVERNANCE DEPARTMENT WITHIN YOUR ORGANISATION.

3.3 Subject Access Requests

Service users have a right to access any information held about them in accordance with the Data Protection Act 1998. If a service user requires access to their personal data which is shared across organisations this will be managed by Leeds City Council. The request should be made to:

cs.freedom.of.information@leeds.gov.uk or can be sent by post to

A76/Freedom of Information Requests
Property, Finance and Technology
Legal, Licensing and Registration
Civic Hall
Leeds LS1 1UR

All communications should include the reference *SLP/EN* to allow the access request to be tracked through the process.

Section 4

Training and staff development

4.1 Information governance and confidentiality training

All staff working under the remit of this agreement (this includes temporary members of staff, volunteers, agency and consultancy staff and students on placement) must have received the appropriate training in information governance and confidentiality and must have appropriate confidentiality clauses in their contracts of employment/service. Each signatory organisation will be expected to provide evidence of this as part of the monitoring of the implementation of the agreement.

4.2 System specific training

All staff will also be required to attend training, provided by their respective organisations, on the electronic systems that they use within service to ensure they have the required level of competency to process and manage data appropriately.

4.3 Training on this ISA

In addition to this, each signatory organisation undertakes to ensure staff working under the remit of this ISA are aware of its existence and the overarching Leeds Interagency Protocol for Sharing Information and that they are trained in its application.

The service will ensure staff working under the remit of this ISA are aware of its existence and the over-arching Leeds Interagency Protocol for Sharing Information and that they are trained in its application. The service will identify a member of staff who leads on information sharing who will be a point of contact for any breaches, reviews or specific work groups relating to the Leeds Substance Misuse ISA.

Compliance with workforce development around the ISA will be monitored through the Safer Leeds Contract Management Process.

Section 5

Dissemination, breaches and complaints relating to this ISA

5.1 Dissemination of this ISA

Partner organisations will disseminate copies of this ISA to all relevant staff and on request to service users and carers. Service users and carers will be offered the Users and Carer leaflet accompanying this agreement. Partners will ensure that appropriate training is provided to all relevant staff.

5.2 Reporting breaches

All reported breaches of the ISA must be logged and investigated and the outcomes reported to the **Information Sharing Steering Group (ISSG)**. The following incidents will be logged:

- Refusal to disclose information
- Conditions being placed on disclosure;
- Disclosure of information to members of staff who do not have a legitimate reason for access;
- Non-delivery of agreed reports;
- Inappropriate or inadequate use of forms e.g. insufficient information provided
- Disregard for procedures
- The use of data/information for purposes other than those agreed in the protocol
- Inadequate security arrangements

If a member of staff is aware of a breach, this should be raised with their line manager. The manager should then make a decision on whether the breach should be dealt with informally within the service, or formally by the ISSG. A breach reporting form is at **Appendix 5**, which will be completed and forwarded both to Safer Leeds Data Systems Co-ordinator and the ISSG.

The ISSG will inform the Safer Leeds Governance Group of any issues to ensure appropriate actions are undertaken by Safer Leeds commissioning team.

5.3 Managing Complaints

If an organisation receives a complaint from a service user with regard to information disclosure, this will be dealt with by the service lead for Information Sharing. The details of the complaint, along with any actions/outcomes taken in investigation, will also be reported to the Safer Leeds Data Systems Co-ordinator.

Section 6 Advice and guidance

This ISA is supported by the Staff guidance document available at the following link <http://www.leedspct.nhs.uk/about/?pagepath=About%20Us/Information%20Sharing/Protocol>

Appendix 1 includes contact details of staff that can provide specialist advice in relation to confidentiality and information sharing issues and relevant additional guidance.

Appendix 1 - Specialist advice contact details

Organisation / individual	Responsibility
Safer Leeds Data Systems Co-ordinator	IT System
Safer Leeds DIP Data Manager	MI-Case
Tom Evans – Leeds Addiction Unit	RESULT

Comment [LU1]: Need S1 contact details and ILLY

Safer Leeds

Advice on information governance issues:

David Reid
Communications and Customer Relations Manager
Service Improvement Section
Leeds City Council

Advice on legal issues:

Legal, Licensing and Registration
Civic Hall
Leeds LS1 1UR

NHS Leeds

Advice on information governance issues: Lara McGuigan, Head of Information Governance: Email: lara.mcguigan@nhsleeds.nhs.uk Tel: 01133057412

Caldicott Guardian: Matt Walsh, Director of Commissioning

Other sources of advice:

- Leeds Inter-Agency Information Sharing Protocol. Copies available at <http://www.leedspct.nhs.uk/about/?pagepath=About%20Us/Information%20Sharing/Protocol>
- The NHS Confidentiality Code of Practice is available at www.dh.gov.uk/jpu/confiden
- A computer-based training package (known as TIGER) covering Data Protection, Caldicott and Information Security. Details available from Pan-Leeds Information Skills Development Group at www.panleedsetd.org.uk
- Confidentiality: Protecting and Providing Information: General Medical Council www.gmc-uk.org
- A GMC booklet includes a list of cases where there is a statutory authority to disclose information in relation to:
 - The Courts including the Coroner
 - Abortion Act and Abortion Regulations 1991
 - Criminal Appeals Act 1995
 - Health and Social Care Act 2001
 - Human Fertilisation and Embryology Act 1990
 - NHS (Venereal Diseases) Regulations 1974
 - Police and Criminal Evidence Act 1984
 - Prevention of Terrorism Act 1989
 - Public Health (Control of Diseases Act) 1984

Appendix 2 - Key principles



The eight principles of the data protection act:

- 1. Fair and lawful:** Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met, also the processing must adhere to the *fair processing code*.
- 2. Use for specified purposes:** Personal data shall be obtained only for one or more specified purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.
- 3. Adequate, relevant and not excessive:** Personal data shall be adequate, relevant and not excessive in relation to the purpose.
- 4. Accurate and up to date:** Personal data shall be accurate and, where necessary, kept up to date.
- 5. Don't keep longer than necessary:** Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.
- 6. Rights given under the act:** Personal data shall be processed in accordance with the rights of the data subject under this act".
- 7. Security:** Appropriate and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- 8. Disclosure outside Europe:** Personal data shall not be transferred to a country outside the European Economic area, without adequate protection.

The six Caldicott Principles:

- 1. Define Purposes:** Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.
- 2. Use anonymised information if possible:** Patient-identifiable information items should not be included unless it is essential for the specified purpose. The need for patients to be identified should be considered at each stage of satisfying the purpose.
- 3. Use the minimum information necessary:** The minimum amount of identifiable information should be transferred or made accessible that is necessary for a given function to be carried out.
- 4. Access to personal information on a need to know basis:** Only those individuals who need access to patient-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. Staff must be aware of their responsibilities:** Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.
- 6. Use only when lawful:** Every use of patient-identifiable information must be lawful.

Appendix 3 - Example leaflet for service users and carers

"How we use your information": A guide for service users and carers

What is this leaflet for?

This leaflet has been produced by organisations providing Substance Misuse treatment services within Leeds Integrated Drug Treatment System. The leaflet gives you details of how we use your personal information and what rights you have.

We have a legal duty to keep personal information confidential. The law allows us to share personal information but only if we follow certain rules. The main law is the Data Protection Act 1998.

What do we mean by personal information?

Personal information is any piece of information which identifies you.

This could include for example:

- Your name
- Your address
- Services you have used or may need
- Details of your physical or mental health
- Details of your social circumstances

Why do we need information about you?

We may need to ask you for personal information so that we can:

- Carry out an assessment
- Develop a care plan
- Make sure you receive the right kind of services

What will we do with your information?

We will keep your information confidentially and securely.

We may need to share this information with other professionals providing services but if we do this we need to follow the rules listed below.

What rules will we follow when we use your information?

- We will tell you why we want information about you
- We will tell you what purpose we want to use it for
- We will only use your personal information where this is necessary.
- We will use the minimum amount of information necessary
- Your information will be kept confidentially and securely
- Your information will be kept accurate and up to date
- Your information will not be kept longer than necessary
- Staff will only have access to your information if they need to in order to carry out their job (i.e. referral, booking of appointments, administration of data systems)
- We will normally ask you for permission to share your personal information*

- We will respect your decision if you choose:
 - Not to share your personal information*
 - To share only some of your information*
 - To share only with some organisations*
- If we need to send your information to other organisations we will do so safely
- We will provide a copy of information we hold about you if requested
- We share some information about you with the NDTMS (NOT full name and address - initials, date of birth, gender and part postcode). This is the database used to collect information on drug and alcohol treatment provision. It is managed nationally by the National Treatment Agency for Substance Misuse (NTA), the NHS body responsible for collecting drug and alcohol data and for overseeing drug misuse treatment in England

*** Please note:**

There are some circumstances where we are allowed to share information without the permission of the service user or carer, for example:

- To protect children at risk of significant harm
- As a duty to the courts
- To protect the service user in a life-threatening situation
- To prevent a crime

Contact us if you need more details about this.

What to do if you need further details?

You may want to?

- Get further details
- See the information we hold about you
- Make a complaint about how your personal information has been used

If so you can:

- Speak to your health or social care professional
- Write to us or phone us using the contact details below
- Email us using the address below

Contact details

*******INCLUDE SERVICES' SPECIFIC CONTACT DETAILS HERE**

Further details are also available from the Information Commissioner which is the Government body responsible for data protection and confidentiality.

Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Tel. 01625 545 745 email mail@ico.gsi.gov.uk

Appendix 4 Informed Consent Form

INFORMED CONSENT

Introduction

It is important to gain your consent to allow us to meet your needs relating to your substance misuse. We will aim to reduce the amount of times you need to repeat information in your treatment journey and we may need to share your information to give you access to a service who can give you support in a specific area (i.e. housing, benefits, etc). You will receive an Information sheet and a copy of this consent to take away with you.

Electronic Data Management System

I consent to my information being held electronically on a **secure** system. At different stages in your treatment, you may want to undertake different activities for support. Your information will then be accessed, when appropriate, by workers delivering the Safer Leeds Treatment and Recovery Service, which consists of:

- Harm reduction services
- Community Drug Treatment Services
- Structured Day Programme
- After-Care
- NFA team
- Specialist services
- Community Rehabilitation & Reintegration Services
- DRR treatment team

This system helps to ensure that treatment services don't need to ask you to repeat information each time you go into a service. Workers **do not** routinely access your information unless they are involved in your care and safeguards are put in place to ensure this.

- I consent to my information being held on the ILLY Care-path system
- I consent to my information being held on System One
- } Worker to include as appropriate

National Treatment Agency (NTA)

The National Drug Treatment Monitoring System (NDTMS) involves collecting information about the type of treatment you receive from a treatment agency. Sometimes you may be seen by more than one agency. Consequently, to avoid duplication of reporting, NDTMS may share a minimal amount of information about you between the agencies from which you may have received treatment.

- Your full name and address are NOT passed on to NDTMS (or the NTA) although some details are sent (e.g. your initials, date of birth, gender and part postcode) to minimise the risk of you being counted twice.
- The NTA does not pass any identifiable information held on the NDTMS to the police or criminal justice agencies.
- Your information is very useful for helping to plan and develop services that can best meet your needs. However, if you do not want information about you to be passed on, you have a right to say this.

I consent to limited information being given to the NTA

Disengagement from services

If we lose contact with you, we will make every effort to keep in touch. That includes us and/or workers in our harm reduction services attempting to contact you. We need to check that you are happy with this.

I consent to a referral to harm reduction services if I disengage from services

I consent to you contacting the following people to try to reach me

Refusal

You have the right to withhold information or pieces of information about yourself that you don't wish to share.

If you do refuse to give consent this may impact upon our ability to provide you with a complete treatment package in the following ways:

- Repeated assessments, care plans and TOPS
- Delays in accessing treatment for you
- Limited ability to provide substitute prescribing

If you are unsure about any of this please speak to your key-worker.

Refusal noted

Withdrawal of consent

You have the right at any time to withdraw your consent about any or all of your information being held or shared within or outside of the treatment system. Please speak to your worker about this should you have any concerns

Families and Carers

It is likely that there are family members or carers who can support you with your treatment. It would helpful for you to think about the family member or close friend who you trust most to give you this support and consider whether you would be happy to have information shared with them about your treatment. If so, please state their relationship to you, their name and contact details.

Services outside of the treatment system

There may be times when we need to share information outside of the treatment system to deliver your support. Please tick the box(es) to indicate consent to share information between agencies:

GP	<input type="checkbox"/>	Social care	<input type="checkbox"/>
Pharmacist	<input type="checkbox"/>	Drug Interventions Programme	<input type="checkbox"/>
Alcohol services	<input type="checkbox"/>	Jobcentre Plus	<input type="checkbox"/>
Mental health services	<input type="checkbox"/>	Prison	<input type="checkbox"/>
Probation	<input type="checkbox"/>	Housing	<input type="checkbox"/>
Courts	<input type="checkbox"/>	Other_____	<input type="checkbox"/>
THINK Family services	<input type="checkbox"/>	Other_____	<input type="checkbox"/>

Signatures

Service user _____

Dated _____

Worker _____

Appendix 5-ISA breach reporting form

Leeds Substance Misuse Services Information Sharing Agreement

Breach of Information Sharing Agreement Reporting Form

Name	Tel. no
Suspected Breach – please provide full details of the suspected breach including what happened, when, who was involved and any action taken. Types of breaches include; <ul style="list-style-type: none">• Refusal to disclose information• Conditions being placed on disclosure;• Disclosure of information to members of staff who do not have a legitimate reason for access;• Non-delivery of agreed reports;• Inappropriate or inadequate use of forms e.g. insufficient information provided• Disregard for procedures• The use of data/information for purposes other than those agreed in the protocol• Inadequate security arrangements	
Passed to	Date
Outcome of investigation – to include brief details of the investigation and any action taken as a result.	
Does the breach need to be reported to the Information Sharing Steering Group Yes / No	
Date reported	
Signed	Date

All formal breaches of this ISA must be notified to the Chair of the ISSG. Email lara.mcguigan@nhsleeds.nhs.uk or Tel: 0113 3057412

Appendix 6 - ISA formal approval form

<p>***** <i>INSERT NAME</i></p> <h2>Information Sharing Agreement</h2>

Approved by:

Designation:

For: E.g. NHS Leeds

Date:

Approved by:

Designation:

For: E.g. Education Leeds

Date:

Copies of this Agreement should be retained by the named persons above and be made available for inspection.

A copy should be sent to the Information Governance Department / Caldicott Guardian of each ISA partner.

Appendix 7

IT System Acceptable Usage Agreement

Scope

This policy covers the use of the Safer Leeds Partnership electronic case management and prescribing system. This agreement applies to all users of, regardless of their employing organisation, their role, or the computer network through which they access the system. This agreement is a subsidiary document of the Leeds Substance Misuse Information Sharing Agreement and all data will be processed in accordance with the document.

The Policy

1. Purpose of the IT system

- Access to the IT system is provided solely for the purposes of case management and prescribing (where applicable) for ADS, Multiple Choice, St Anne's Harm Reduction, Barca Harm Reduction, the Leeds Community Drugs Partnership (LCDP), St Martin's Healthcare Services and T3.
- You must not access or use information from the system for any other purpose.
- You must not access, or attempt to access the system outside of your business hours, or from non-business premises unless otherwise agreed with your manager and the Data Systems Co-ordinator at Safer Leeds.
- You must comply with the system operating procedures and working instructions.

2. Access Monitoring

- Your actions on the system will be recorded and monitored as part of the routine administration and management of the system.

3. User Security

- You must keep your user logon details confidential.
- You must not allow anyone else to use your logon.
- You must never log onto the system using someone else's logon.
- If you believe your logon has been used by someone else you must report this to the Data Coordinator at Safer Leeds immediately. Your password will be changed as soon as possible.

4. Information Security

- You must keep information on the system confidential and only share it where permitted to facilitate the service user's care pathway.
- You are responsible for ensuring that information you add to the system is accurate.

- IT Systems must not be used for preparing, storing, receiving, displaying, transmitting or communicating information, material or messages:
 - that are inconsistent with the mission or values of your parent service
 - that may have the effect of harassment of any person or
 - that may be defamatory.
 - This includes, but is not limited to pornography, racism, sexism, homophobia, obscenities, insults, threats and intimidation.
- You must virus-scan all documents before they are uploaded to the system as attachments in the Documents section.
- You must not disclose details of system security or administration procedures to any unauthorised person.

5. Breaches of this agreement

- Any suspected breaches of this agreement will be reported to your employing organisation, and will be handled through the relevant disciplinary procedures.
- System access may be suspended temporarily or permanently as part of this process.

Agreement

I have read and understood this agreement, and agree to abide by its terms.

I will abide by all the principles of the Data Protection Act 1998, the Computer Misuse Act 1990 and the Official Secrets Act 1989.

This agreement applies until further notice, but users will be asked to re-sign every 2 years.

Person requesting access to IT Case Management Systems	
Name	
Role	
Organisation	
Signature	
Date	