INFORMATION SHARING AGREEMENT

WEST YORKSHIRE POLICE

and

LEEDS AND YORK PARTNERSHIP NHS FOUNDATION TRUST

Version 4.0

CONTENTS

SUMMARY SHEET
1. INTRODUCTION
2. PURPOSE
3. PARTNER(S)
4. POWER(S)
5. PROCESS
6. DATA QUALITY
7. INFORMATION SECURITY
8. COMPLAINTS & BREACHES
9. AMENDMENTS TO THE AGREEMENT
10. SUBJECT ACCESS
11. FREEDOM OF INFORMATION
12. SIGNATURE
13. CONTACT DETAILS

Appendix A: Request for disclosure of information form

Appendix B: A Guide to the completion of ISA Information Request Form

SUMMARY SHEET

West Yorkshire Police & Leeds and York Partnership NHS Foundation Trust

PURPOSE	To provide Leeds and York Partnership NHS Foundation Trust (LYPFT) with specific West Yorkshire Police information, in an appropriate and lawful manner. To ensure the best possible service is provided to persons who are mentally ill and to ensure the safety of those service users, employees of each organization and the public as a whole.

Partners	West Yorkshire Police & Leeds and York Partnership NHS Foundation Trust

Date agreement comes into force:	14/03/2012

Date of Agreement Review:	Reviewed annually

Agreement Owner:	West Yorkshire Police – Information Management

Agreement Drawn up by:	David Mason – Data Protection Manager West Yorkshire Police Jeanette Lawson – Clinical Operations Manager Crisis Resolution Home Treatment Service/Acute Community Services – LYPFT

Location of Agreement in Force:	West Yorkshire Police – Information Management LYPFT – Staffnet Information Sharing Agreements

Protective Marking:	Not Restricted

VERSION RECORD

Version No.	Amendments Made	Authorisation
1.0	First Draft	David Mason/Jeanette Lawson
2.0	Update WYP contact details	Jeanette Lawson/Mick Hunter
3.0	Update LYPFT organization name and annual review	Jeanette Lawson/Mick Hunter
4.0	Update SPOC and ISA form wording, addition of guide to ISA completion, change of information storage.	Dan Jones/Jon Mellor/Paul Hobson

1. INTRODUCTION

1.1 Since the inception of the Section 136 service in April 2007 Leeds and York Partnership NHS Foundation Trust (LYPFT), West Yorkshire Police (WYP) and other partnership agencies have operated within guidelines outlining the manner in which persons detained under Section 136 of the Mental Health Act in Leeds should be dealt with. Underpinning the guidelines is the desire to ensure that persons who are mentally ill are treated promptly and effectively in accommodation suitable for that purpose.

1.2 Since that time it has become increasingly apparent that LYPFT require information regarding any person who comes under their care in order to prevent criminal activity against staff and other service users.

2. PURPOSE

2.1 The purpose of this agreement is to establish a lawful, efficient and consistent method of disclosing appropriate, quality information to LYPFT for them to meet their statutory requirements.

2.2 This agreement will detail what information is to be provided with the request and to what standard that information should be. Also included will be the performance and statutory drivers that influence the frequency and time constraints of the request.

2.3 The agreement has been made in accordance with the Leeds Interagency Protocol for Sharing Information.

3. PARTNER(S)

3.1 This agreement is between the following partners only:

3.2 West Yorkshire Police and Leeds and York Partnership NHS Foundation Trust.

3.3 It will be the responsibility of these partner(s) to ensure that:

- Realistic expectations prevail from the outset
- Ethical standards are maintained
- A mechanism exists by which the flow of information can be controlled
- The integrity of the data is maintained and protected at all times
- Appropriate training is given (Data Protection Act awareness / handling of sensitive personal data)
- Adequate arrangements exist to test adherence to the Agreement

4. POWER(S)

4.1 This agreement has been prepared with the obligations of the

statutory guidance, the "Management of Police Information" (MoPI) in mind. Section 6 of MoPI provides standards that must be applied by West Yorkshire Police when sharing information with external agencies. This ISA is compliant with such standards.

This agreement relies upon the following legal powers:

- The Human Rights Act 1998 (article 2 & 8); and;
- The Data Protection Act 1998 (see below) & (sec 29(3) & 35(2)(a)(b)
- Common Law Powers of Disclosure
- Crime and Disorder Act 1998 (Section 115)

4.2 Data Protection Act 1998 Fair Processing – Legitimate Expectation
Information shared by WYP to LYPFT will **only** be used to satisfy a policing purpose and in strict accordance with MOPI (Police Act 1996). It is justifiable for the Police to hold that those persons who supply information to the Police or who have information about themselves held by the Police will expect it to be used for a legitimate policing purpose.

4.3 Compliance with at least one condition in Schedule 2 - DPA
Where WYP will share personal information for the purpose of this agreement, the Chief Constable (as data controller) will be exercising a function conferred under the above identified legislation and therefore complying with Schedule 2 (DPA) Para 5(a)(b).

4.4 Compliance with at least one condition in Schedule 3 - DPA
Where WYP will share SENSITIVE personal information for the purpose of this agreement, the Chief Constable will be exercising a function conferred under the above identified legislation and therefore complying with Schedule 3 (DPA) Condition 7(a)(b).

5. PROCESS

5.1 This agreement has been formulated to facilitate the exchange of information between Partners. It is, however, incumbent on all partners to recognise that any information shared must be justified on the merits of each case (on a case by case basis).

5.2 **Types of Information to be Shared:**
West Yorkshire Police will share:

- Personal details including name, address, date of birth, custody reference number (if applicable) and medical or risk issues of any person under the care of LYPFT. Issues will include details of any relevant convictions, any relevant previous risk assessments.

- Statistical data – information that can be considered relevant to the provision of facilities to Section 136 detainees in West Yorkshire such as arrest data including localities and times.

- Operating guidance as agreed between LYPFT, West Yorkshire Police and other partner agencies.

***Leeds and York Partnership NHS Foundation Trust will share*:**

- Information from assessments that is relevant to the purpose of this agreement (Sections 1 and 2).

- In respect to those detained under Section 136 not admitted to hospital details of where those persons are placed within the community.

- Any identified risks that become apparent during the examination / treatment of the detainee.

- Management information data to include assessment times, diagnosis (if available) and outcome.

- Copies of any forms completed and signed by police officers required for the purposes of any criminal or civil proceeding.

5.3 **Constraints on the Use of Information:**

5.3.1 All organisations Data Protection Officer / Manager / Information Managers / Chief Executives **must** be fully aware of their own obligations under the Data Protection Act 1998 regarding the handling of data / loss of data **(All losses of West Yorkshire Police data by LYPFT MUST be reported to the Police Single Point of Contact (SPoC) and Police Data Protection Manager).**

5.3.2 The information shared must not be disclosed (via copy or actual documentation) to any third party and must not be used or disclosed for any other purpose (without the express permission of the Chief Constable of West Yorkshire Police).

5.3.3 Information must be stored securely and destroyed when it is no longer required for the purpose for which it is provided. Partner organizations will ensure records retention and disposal is aligned to organizational and/or sectoral guidelines.

5.3.4 Disclosure of personal data must be relevant and only the minimum amount required for the purpose should be used for the purpose for which it is supplied. INFORMATION MUST NOT BE DISCLOSED "JUST IN CASE" IT IS REQUIRED (Third Principle DPA & the Caldicott Principles).

5.3.5 The identity of the originator must be recorded against the relevant

data. No secondary use or other use may be made unless the consent of the disclosing party to that secondary use is sought and granted in writing (see 5.2.2).

5.3.6 Disclosure of personal information should only be made provided that it can be demonstrated that it is required for a policing purpose as defined in the Code of Practice for the Management of Police Information (MoPI), e.g.

- Protecting life & property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice
- Any duty or responsibility arising from common or statute law

Please note the ISA does NOT cover the release of intelligence or investigation details. Please be specific about why you are requesting the information.

5.3.7 Disclosure must be compatible with the second data protection principle:

- "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes"

5.3.8 Disclosure must be compatible with the Caldicott Principles, namely that:

- We can justify the purpose(s) of using person-identifiable and sensitive information
- We only use person-identifiable and sensitive information when absolutely necessary
- We use the minimum information that is required to achieve the desired purpose(s)
- Access will be on a strict need-to-know basis
- Everyone must understand his or her responsibilities
- Everyone understands and complies with the law
- We recognise that the duty to share information can be as important as the duty to protect patient confidentiality

5.4 Roles and Responsibilities under this Agreement:

5.4.1 The sharing of information must only take place where it is valid and legally justified.

5.4.2 Each partner must appoint a Single Point of Contact (SPoC) who must work together to jointly solve problems relating to receiving the information and its processing. Whenever the SPoC changes, each partner should be informed and, if necessary, the ISA updated. The roles and responsibilities of the SpoCs must be clearly defined for each of the partners (in line with MoPI Appendix 3 - 5.4.1).

5.4.3 SPoCs should meet regularly to discuss how the agreement is working. All contacts have a responsibility to create a file or folder (electronic or otherwise) that can record each individual request for information and the decision made. It must include copies of the request for information, details of the data accessed and notes of any meeting, correspondence or phone calls relating to the request.

5.4.4 Any request for personal information must meet one or more of the policing purposes (in accordance with DPA Schedule 2 & 3 – see 4.3 & 4.4).

5.4.5. Within West Yorkshire Police, the ISA must be held and managed centrally by the Data Protection Manager. Any other documentation (e.g. the Request for disclosure of information form) must be held by the SPoC. This arrangement must be mirrored between the partners.

5.4.6 The designated Police SPoC must ensure that the request for personal information meets a policing purpose as specified in the Code of Practice for Managing Police Information (MoPI).

Partner	**Job Title of SPoC**
West Yorkshire Police	Force Disclosure Unit
Leeds and York Partnership NHS Foundation Trust	Risk Management Department

5.5 Specific Procedures:

5.5.1 Handling requests for information – Where regular (e.g. daily, weekly, monthly) requests for information are processed within the terms of the agreement, it is the responsibility of the SPoC to keep a log of the dates, data sent, requestor, etc. Any requests for personal information under this agreement must be made in writing using the 'Request for Disclosure of Information Form' (Appendix A). All sections of the form must be completed and must show an authorised signatory prior to being directed to a nominated officer.

5.5.2 A guide to the completion of this form is found in Appendix B

5.5.3 Requests from LYPFT will be from Clinical Team, Operational or Service Managers or from Consultant Psychiatrists. All e-mailed requests must be sent to:

rm-policeinfo.LYPFT@nhs.net

5.5.4 Staff will be able to contact the Trust's Single Point of Contact (SPoC) Dan Jones based at Trust HQ - 07949 102101 - for any query as to the current position re the Information Sharing Agreement or any individual request.

5.5.5 **Any message containing personal information will not be sent via non-secure e-mail. Information will only be**

transferred by e-mail when there is clear evidence of a secure (at least to 'Restricted' level) network in place. The circulation of police information must follow the guidance laid down in the Government Protective Marking Policy, which can be found on the West Yorkshire Police Policy database. Personal information and sensitive personal information should be exchanged between Government Secure Intranet (GSi) e-mail addresses when available or alternatively by other secure method. Your organisation Data Protection Officer / Information Security Officer or equivalent will be able to advise.

5.5.6 Responses by West Yorkshire Police Staff to URGENT requests must be performed as soon as is reasonably practicable and subject to local negotiations. All other requests will be completed ten (10) working days as agreed (subject to constraints placed on WYP staff, namely that the Information Technology (IT) and PNC systems are operational at the time).

5.5.7 Responses from West Yorkshire Police Staff will be e-mailed to the LYPFT SPoC who will then input the data into PARIS via the third party sensitive casenote tab. An alert will be placed on the record stating there is Police ISA information available. This information must not be disclosed to the service user under any circumstances and the casenote will carry a clear warning referencing this.

5.5.8 The SPoC will notify the initial requestor via e-mail that information has been received and updated to PARIS and reminding the requesting clinician to update risk assessments accordingly. A read receipt will be requested regarding this. If the read receipt is not received within 3 days, this will be escalated to the requestor's service manager, to ensure staff are aware of the ISA data on the service users file.

5.5.8 **Regular audits** of the information exchanged should be undertaken by the SPoC to ensure that they contain details of the decisions made and that the decisions to share information have been made in accordance with the agreement, Data Protection principles and for a legitimate policing purpose. (As defined in MoPI) The Information Management Department and the Force Data Protection Manager will plan and perform audits as required. The auditing has been built into a 1-year audit plan and will be performed when necessary.

5.5.9 ISA information on PARIS MUST be removed under a subject access request once the casenotes have been received by medical records. This is the responsibility of the clinician who is checking the records before disclosure.

5.5.10 The front sheet to the subject access request from medical records will clearly indicate where the record contains information gained under the ISA, and the clinician responsible for removing sensitive data must sign and return this form to medical records, as per the

subject access request policy.

5.5.11 The SPoC for LYPFT will maintain an up-to-date record of all ISA requests made, in connection with medical records.

5.6 Review, Retention and Deletion

5.6.1 Partners to this agreement undertake that personal information shared will only be used for the specific purpose for which it is requested and not forwarded to other third parties without the consent of the data controller. ***The recipient of the information is required to keep it securely stored and it will be confidentially destroyed when it is no longer required***.

5.6.2 The recipient will not release the information to any third party without obtaining the express written authority of the partner who provided the information (Data Controller – Chief Constable of West Yorkshire Police)

5.7 Review of Information Sharing Agreement

5.7.1 The ISA will be monitored annually by the WYP SPoC and the partner SPoC. The nominated holder of this agreement is West Yorkshire Police. It is based on the national template for information sharing which forms part of the guidance issued on the Management of Police Information by ACPO and the Home Office.

5.8 Indemnity

5.8.1 All partners as receivers of police information will accept total liability for a breach of this Information Sharing Agreement should legal proceedings be served in relation to a breach of data protection or other legislation in which the partner organisations staff, associated personnel or systems are culpable in the breach.

6. DATA QUALITY

6.1 Information discovered to be inaccurate or inadequate for the purpose will be notified to the data controller who will be responsible for correcting the data and notifying all other recipients of the data who must ensure that the correction is made.

6.2 Any disclosure of personal data must have regard to both common and statute law e.g. defamation, the common law duty of confidence and data protection principles as well as any relevant codes of practice and Human Rights.

7. INFORMATION SECURITY

7.1 Signatories to this agreement must designate an individual or individuals within their organization to assume responsibility for data protection, security and confidentiality and compliance with

legislation. A designated person will ensure that Data Protection Registrations or notifications are in place to cover the holding and use of personal data.

7.2 It is expected that partners of this agreement will have in place baseline security measures compliant with BS7799:2005 and ISO/IEC 27001:2013 and HMG standards in relation to information security, or similar standards as mandated by sectorial frameworks such as the HSCIC IG Toolkit, etc.

7.3 All signatories will ensure that they have these appropriate security arrangements in place. Only nominated representatives can access, request information, and make disclosure decisions. Data should be stored securely to prevent unauthorized access and disclosure.

7.4 The Information Security Officer from West Yorkshire Police will, by arrangement, undertake a physical review of the security in place to ensure the confidentiality, integrity, availability and non-repudiation of the Force information being stored under this agreement.

8. COMPLAINTS AND BREACHES

8.1 Complaints from data subjects, or their representatives, regarding information held by the Partnership will be investigated first by the organization receiving the complaint. Action that affects other signatories will not be taken without the consent of all parties to this agreement.

8.2 Breaches of information security, subject confidentiality or access controls regarding the information held by the Partnership will be investigated first by the organization whose security has been breached. Action that affects other signatories will not be taken without the consent of all parties to this agreement.

8.3 Partner organizations will have robust policies and procedures relating to confidentiality, information security and access controls which will be shared with partners on request.

9. AMENDMENTS TO THE AGREEMENT

9.1 Any partner may make suggestions for amendments to the agreement at any time.

9.2 To enable partners to exchange views prior to changes being made it is suggested that such changes be discussed at the appropriate forum. No changes can be made unless each is agreed

10. SUBJECT ACCESS

10.1 When an agency receives a subject access application and personal data is identified as belonging to another agency, it will be the responsibility of the receiving agency to contact the data controller

to determine whether the latter wishes to claim an exemption under the provisions of the Data Protection Act 1998.

10.2 Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless: -

a) The other individual has consented to the disclosure of the information to the person making the request, or,

b) It is reasonable in all circumstances to comply with the request without the consent of the other individual.

10.3 In determining whether it is reasonable, regard should be had to:

- Any duty of confidentiality owed to the other individual.
- Any steps taken by the data controller with a view to seeking the consent of the other individual.
- Whether the other individual is capable of giving consent, and
- Any express refusal of consent by the other individual.

11. FREEDOM OF INFORMATION

11.1 The Freedom of Information Act 2000 gives people the right to request information from public authorities or any publicly-funded organization. In each publicly-funded organization's Freedom of Information Publication Scheme on their Internet site, details of how to contact the Freedom of Information Officers are given. Requests must be passed to that Officer in the first instance.

- In publicly-funded organizations, that officer will handle the request.
- In non-statutory organizations, the request must be passed to the appropriate Manager or Chair of the partnership

Should a Freedom of Information Act request be received, before a response is finalized and released to the requester, ALL interested parties will be informed as to the likely response and their views sought.

12. SIGNATURES

12.1 By signing this agreement, all signatories accept responsibility for its execution and agree to undertake a level of training of staff that ensures that requests for information and the process of sharing itself is sufficient to meet the purpose of this agreement.

12.2 Signatories must also ensure that they comply with all relevant legislation.

Organisation	Representative	Position Held	Signature
West Yorkshire Police	Michael Hunter	Chief Inspector	Signed
Leeds and York	Jim Isherwood	Caldicott	Signed

Partnership NHS Foundation Trust		Guardian Medical Director	

13. CONTACT DETAILS

Name	Organisation	Position Held	Email & Telephone
Dan Jones	Leeds and York Partnership NHS Foundation Trust	SPOC & Local Security Management Specialist	rm-policeinfo.LYPFT@nhs.net 07949102101
Paul Hobson	West Yorkshire Police	Detective Inspector	paul.hobson@westyorkshire.pnn.police.uk 0113 3852824
Carl Starbuck	Leeds and York Partnership NHS Foundation Trust	Information & Knowledge Manager (DPA / FoIA Officer)	Carl.starbuck@nhs.net 0113 855 9771

APPENDIX A

Link to blank ISA form

APPENDIX B

Link to guidance for completion of ISA form