NHS
Stockport
NHS Foundation Trust

Information Sharing & Transfer of Records Policy

State whether the document is: ☑ **Trust wide**	**State Document Type:** □☑ **Policy**
APPROVAL **VALIDATION**	Information Governance & Security Group Finance & Performance Committe
DATE OF APPROVAL **DATE OF VALIDATION**	May 2018 June 2018
INTRODUCTION DATE	
DISTRIBUTION	Information Governance & Security Microsite
REVIEW	**Original Issue Date** March 2006 **Review Date** June 2020
CONSULTATION	Information Governance & Security Group
EQUALITY IMPACT ASSESSMENT	☑ **Screening** ☒ Initial ☒ Full
RELATED APPROVED TRUST DOCUMENTS	Information Governance Policy Information Governance Strategy Information Security Policy Information Security Incident Reporting/Management IT Acceptable Use Policy Mobile Devices & Removable Media Security Policy Remote Access & Mobile Working Policy Photography/Video & Audio Records of Patients/Staff Network Security Policy Data Protection & Confidentiality Policy Access to Personal Information (Subject Access) Policy Data Quality Policy Freedom of Information Policy Records Management Policy Records Management Strategy Disciplinary Policy Incident Reporting SOP Inquest Policy
AUTHOR/FURTHER INFORMATION	Khaja Hussain Assistant Director Information Governance & Security
VERSION NUMBER	Version 6.1
THIS DOCUMENT REPLACES	Version 6.0 (Jun 2018)

Document Change History:

Issue No	**Page**	**Changes made** (include rationale and impact on practice)	**Date**
6.1	*9*	*Clarification on sending information via the internal mail (specifically to take account of staff working in the community)*	*Aug 2018*
6.0		*GDPR inclusion*	*May 2018*
5.0	*Multiple* *6* *9*	*Refresh of Policy* *Clarification of Secondary Use purpose* *Clarification of procedure when using royal mail*	*April 2017*
4.3	*6, 10, 13*	*Clarification over secondary use requirements* *Update to secure e-mail domain information* *Clarification around sharing PID internally*	*Oct 2015*
4.2	*10 and 13*	*Updated to include information on posting health records; information security when transporting information off site*	*July 2015*
4.1	*12* *15*	*Updated information relating to NHS encryption facility* *Inclusion of Secure File Transfer information*	*March 2015*
3.1	*6,7,12*	*Included definitions for primary and secondary uses, pseudonymisation, responsibility of Information services department and a section on pseudonymisation process*	*May 2014*
3.0	*16 - 23*	*Renamed to clarify scope, previously Information Sharing & Safe Haven Policy. ISP reviewed.*	*February 2013*
2.2	*14, 16*	*Minor alterations to leaflet and ISP.*	*September 2011*
2.1	*9*	*Inclusion of further detail in relation to NHS mail and clarification of where encryption should be applied manually.*	*September 2011*
2.1	*4*	*Section 2 - Inclusion of first paragraph for clarification around the scope of the document. Other minor amendments to wording.*	*September 2011*
2.0 (Final)	*15-17*	*Inclusion of an Information Sharing Protocol template at appendix (b)*	*March 2011*
2.0 (Draft)	*Multiple*	*Adopted the new Trust Policy format.* *Significant Changes Made.* *Including inclusion of definitions; requirements around telephones, transportation and whiteboards; change to the official Safe Haven location; further details of the legal requirements of information sharing and; implementation and monitoring arrangements.*	*January 2011*
1.2	*Multiple*	*Significant Changes Made.*	*October 2008*
1.0		*New Policy*	*March 2006*

Contents

1. INTRODUCTION

All NHS organisations require safe haven procedures to maintain the privacy and confidentiality of the personal information held. The implementation of these procedures facilitates compliance with the legal requirements placed upon the organisation.

Where departments within the Trust, other NHS Trusts or other agencies want to send personal information to a Trust department, they should be confident that they are being sent to a location which ensures the security of the data.

The details of every NHS Trust's safe haven point are listed in the National Safe Haven Directory.

A number of Acts and guidance dictates the need for safe haven arrangements to be set in place, they include:

Data Protection Act 1998 (Principle 7): "*Appropriate technical and organisational measures shall be taken to make personal data secure"*

Confidentiality: NHS Code of Practice 2003: Annex A1 Protect Patient Information *"Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are secure as they can be"*

Further information can be found on the **Information Governance and Security** microsite on the Trust Intranet, which has up-to-date polices, guidance and codes of practice. Detailed procedures for each method of transfer are available on this site. This policy should be read in conjunction with these procedures.

2. STATEMENT OF INTENT / SCOPE OF THE POLICY

This policy applies to Stockport NHS Foundation Trust, referred to as the 'Trust', and includes all hospitals, units and community health services managed by Stockport NHS Foundation Trust.

This policy provides:

- The legislation and guidance which dictates the need for a safe haven.
- A definition of the term safe haven.
- When a safe haven is required.
- The necessary procedures and requirements that are needed to implement a safe haven.
- Rules for different kinds of safe haven.

The processes described in this policy must be followed by all Trust staff, unless exceptional circumstances arise, which may have an impact on direct patient care and when advice/guidance has been sought.

This policy applies to all those working in the Trust, in whatever capacity. A failure to follow the requirements of the policy may result in investigation and management action being taken as considered appropriate.

This may include formal action in line with the Trust's disciplinary or capability procedures for Trust employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non-compliance may also lead to criminal action being taken.

The Trust will also be subject to the General Data Protection Regulations when they come into force on 25th May 2018.

3. SUMMARY

This document and associated policies and procedures identify the principles required to ensure that all staff comply with the law and best practice when handling information and to ensure that information is shared in an appropriate manner and secured in transit.

4. DEFINITIONS

4.1 Safe Haven:

The term safe haven is a location situated on Trust premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely. In a Trust they are the point from where person identifiable data is controlled.

The official designated safe haven location in Stockport NHS Foundation Trust is:

Stockport NHS Foundation Trust
Room 19, Information Department
2nd Floor, Cedar House
Stepping Hill Hospital
Poplar Grove, Stockport
SK2 7JE

Tel: 0161 419 5407
Fax: 0161 419 5304

All staff should be aware of this location, especially as some calls, fax and mail are directed to the listed safe haven only.

However, any department sending, receiving, holding or communicating person identifiable data, concerning either patients or staff, should provide safe haven conditions by following the guidelines set out within this policy.

4.2 Person Identifiable Information / Data (PID):

This is also referred to as, “personal / confidential information” and relates to information about a person which would enable that person’s identity to be established by one means or another.

This might be fairly explicit such as an unusual surname or isolated postcode or bits of different information which if taken together could allow the person to be identified.

All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent. This includes the nationally recognised NHS number.

4.3 Sensitive Information:

This is information where loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community.

This is wider than, but includes, data defined as sensitive under the Data Protection Act 1998. In addition to personal and clinical information, financial and security information is also likely to be deemed “sensitive”.

Examples of sensitive information include information in relation to a person’s:

- Health or physical condition
- Sexual life
- Ethnic origin
- Religious beliefs
- Political views
- Criminal convictions
- Trade Union Membership

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

4.4 Primary and Secondary uses of Information

Primary Use (Direct Care) – is when information is used for direct healthcare and medical purposes. This would directly contribute to the treatment, diagnosis or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided.

Secondary Use (Non-Direct Care) – is when information is not used for direct healthcare and medical purposes. Generally this could be for research purposes, audits, service management, commissioning, contract monitoring and reporting facilities. PID should not be used for secondary use purposes so any data shared **must be** limited and de-identified using anonymisation or pseudonymisation techniques.

4.5 Anonymised or Pseudonymised Information

This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity.

Anonymisation - requires the removal of name, address, full postcode, NHS Number and any other detail or combination of details that might support identification.

Pseudonymisation - requires replacing person identifiers in a dataset with other unique values (pseudonyms) from which identities of individuals cannot be inferred, e.g. the replacement of an NHS number with another random number. Pseudonymisation may be reversible or irreversible

4.6 Portable Electronic or Removable Media:

This includes tapes, floppy discs, laptops & Tablets, optical discs - DVD & CD-ROM, solid state memory cards, memory sticks, Smartphones and pen drives.

4.7 Information / Data Flow / Information Flow Mapping

This is the process of documenting the flow of information from one physical location to another and the method by which it “flows”. Data flows may be by: Verbal transfer, E mail, fax, post/courier, text, or portable electronic or removable media.

4.8 Information Sharing Protocol

The Information Sharing Protocol (Appendix b) should be used with Health and Social Care Organisations and Partners. It sets out general principles with which both parties must comply at all times. It specifies the categories of data that will be shared and the purpose(s) for which the recipient is permitted to use each category of data, including specific security measures that the parties shall put in place to protect the data. It must be signed the Caldicott Guardian or authorised senior officer of each organisation.

4.9 Confidentiality Agreement

This agreement should be used by contractors or third party suppliers of information systems and services, including support, maintenance or consultancy where the third party may have access to person identifiable or sensitive data on-site, or off-site (including remote access).

5. ROLES & RESPONSIBILITIES

5.1 Chief Nurse / Caldicott Guardian:

The Caldicott Guardian is the Trust's Director of Nursing & Midwifery. The Caldicott Guardian has responsibility for safeguarding the confidentiality of patient information.

5.2 Information Governance Team / Assistant Director of Information (Information Governance & IT Security):

The Information Governance Team are responsible for coordinating improvements in data protection, confidentiality and information security.

5.3 Information Governance Department

As the official designated safe haven location in Stockport NHS Foundation Trust, the Information Governance team will ensure that appropriate safe haven processes are in place. For secondary use, the information team will ensure that any queries and reports produced will be effectively anonymised, where appropriate, and suitably encrypted when anonymisation is not possible.

5.4 All Trust Managers:

Managers within the Trust are responsible for ensuring that the policy, and other associated policies and supporting standards and guidelines are built into local processes and that there is on-going compliance.

Managers are accountable for the communication about and compliance with Trust policies, and must ensure that staff are adequately trained and apply the appropriate guidelines.

5.5 All Trust Staff:

All staff, whether permanent, temporary or contracted are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

All staff are responsible for any records or data they create and what they do with information they use.

Staff should ensure they attend information governance training and awareness sessions to maintain their knowledge and skills.

All staff have a responsibility to adhere to information governance standards which are written into the terms and conditions of their contracts of employment.

All staff that process personal-identifiable information and managers who have responsibilities for those staff must ensure that they abide by this policy.

6. THE POLICY

6.1 Requirements for Safe Havens

6.1.1 Location/Security Arrangements:

- Any area sending/receiving person identifiable information should consider the physical security arrangements i.e. a room that is locked or preferably accessible via a coded key pad known only to authorised staff, this key pad should be in use at all times. This should be the first step in the aim to create safe haven conditions.

- The office or workspace should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to any member of staff who work in the same building or office, or any visitors.

- If sited on the ground floor, any windows should have locks on them.

- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.

- Manual paper records containing person-identifiable information should be stored in locked cabinets, where possible.

- Computers should not be left on view or accessible to unauthorised staff and the screen ‘locked’ (using Ctrl, Alt, and Delete keys simultaneously / windows and ‘L’ key) or be logged/switched off when not in use.

- Equipment such as fax machines in the safe haven should have a coded password and be turned off out of office hours.

- Confidential information should not be removed from a safe haven office unless absolutely necessary.

- Operate a clear desk policy, especially when hot desking or working in an open plan office.

6.1.2 Fax Machines:

Fax machines must only be used to transfer personal information **where it is absolutely necessary** to do so. The following rules must apply:

- The fax is sent to a safe location where only staff that have a legitimate right to view the information can access it.

- You notify the recipient when you are sending the fax and ask them to acknowledge receipt.

- The sender is certain that the correct person will receive it and that the fax number is correct.

- Care is taken in dialling the correct number, and pre-programmed numbers are used, where possible.

- Confidential faxes are not left lying around for unauthorised staff to see.

- Only the minimum amount of personal information should be sent, where possible the data should be made anonymous or a unique identifier used.

- Faxes sent should include a front sheet, which contains a suitable confidentiality clause/disclaimer, and states who the information is intended for.

- Where possible, Personal details, i.e. patients name and address, should be faxed separately from clinical details; both transmissions should be accompanied by the NHS number.

- A report sheet is printed to confirm that the transmission was successful (this does not however confirm receipt). The details of this report should be double checked to ensure that they are accurate.

6.1.3 Communication by Post:

- All sensitive records must be placed face down in public areas and not left unsupervised at any time.

- Incoming mail should be opened away from public areas.

- Outgoing mail (both internal and external) should be sealed securely in robust envelopes and marked ‘private and confidential’ or ‘private and confidential - to be opened by addressee only’ (if the information is particularly sensitive or intended for a particular individual). Where possible use tamper-evident envelopes or tape/seals.

- Where sending bulk personal/sensitive information – such as a medical record - use recorded/registered delivery or secure courier services. This is not necessary when sending single sheets such as appointment letters, however care must be taken to ensure that only the name and address is visible and that no personal information can be viewed through any window envelopes.

- Confirm the name, department and full address of the recipient before sending any information out, and ask the recipient to confirm receipt.

- Ensure information is sent to a safe location.

- Under no circumstances should patient information be sent in the internal mail, across the Stepping Hill site. For staff who need to transport information from site to site (in particular staff working in the community), it is acceptable to transport via the internal mail however such staff will be responsible for ensuring:

(a) the information is transported in a secure/robust, adequately sealed envelope, and
(b) Accurate tracking information is recorded (to include the date the information is put into the postal system; the location of the pick-up point i.e. where the outgoing post-tray is located; the name, address and job-title of the recipient
(c) Recipients contact the sender to confirm receipt, to allow the tracking information to be updated

6.1.4 Computers:

- Access to any PC must be password protected; passwords must not be shared, written down or disclosed in any way.

- Computer screens must not be left on view so members of the general public or staff, who do not have a justified need to view the information, can see personal data.

- PCs or laptops not in use should be logged/switched off or the screen 'locked' (using Ctrl, Alt, and Delete keys / windows and 'L' key) when not in use.

- Information should be held on the Trust's network shared or home drives/servers, for example 'I' drive, 'J' drive or 'S' drive and **not** stored on local computer hard drives i.e. 'C' drive (usually 'my documents'). Departments should be aware of the high risk of storing information locally and take appropriate security measures e.g. Encryption and Back-Up Procedures.

- Confidential Information stored on network shared drives should be restricted as appropriate. IT services can assist in establishing folder access rights.

- Undertake regular house-keeping of your files, ensuring only the minimum amount of data is retained, in accordance with the Trust's Records Management Policy and NHS Records Management Code of Practice Retention Schedules.

- The Information Governance Team must be informed of any new database/system applications created/introduced that contain person identifiable information.

- Any database, containing personal information should comply with the Data Protection Act Principles and the Caldicott Principles.

6.1.5 E-mail:

Great care should be taken in sending personal information, especially where the information may be of a clinical nature – it should be encrypted and procedures undertaken to ensure that the correct person has received it.

Email should only be used to send person identifiable information if absolutely necessary, appropriately authorised and encrypted to the appropriate standard.

NHS mail (@NHS.net) automatically secures data sent to other @nhs.net email address or any of the following secure email domains.

NHS
NHSmail (*.nhs.net)
Central Government
xGSI (*.x.gsi.gov.uk)
GSI (*.gsi.gov.uk)
GSE (*.gse.gov.uk)
GSX (*.gsx.gov.uk)
CJX (*.pnn.police.uk *.cjsm.net)
SCN (*.scn.gov.uk)
Local Government
GCSX (*.gcsx.gov.uk)

NB: *.gov.uk and *.police.uk alone are not secure domains. The email address must contain one of the domains above IN FULL.

It is important to note that mail sent from NHS mail (@NHS.net) to any other email domain including (@stockport.nhs.uk) is not secure and should not be used for transferring person identifiable information. Data sent from @stockport.nhs.uk to @NHS.net is also unsecure and should therefore not be used to transfer person identifiable or confidential information without encryption.

- All personal information sent by e-mail should be encrypted to NHS cryptographic standards (currently 256bit strength). The Trust has an email encryption facility (Trend Micro) that can be used to send information securely when using Stockport NHS Foundation Trust's local email system i.e. @stockport.nhs.uk, and where the use of NHS mail is not possible.

  Encryption must be applied manually by typing **[secure]** (including the square brackets) in the subject header of the e-mail message. Further guidance can be found on the IG & Security microsite.

- In addition to the Trust's own encryption facility, NHS mail has also introduced a facility to enable identifiable information to be sent to non-secure e-mails, that is encrypted to the required standard. Guidance is available on the Information Governance & Security Microsite, E-mail and E-mail Encryption page.

- Where possible, only send personal information over NHS mail (@NHS.net to @NHS.net) i.e. when communicating with other NHS organisations also using NHS mail.

- Emails are sent to the right people. Confirm the intended email address before sending and ask the addressee to acknowledge receipt.

- The receiver is ready to handle the information in the right way.

- Clinical information should be clearly marked.

- Person identifiable information should not be written in the 'subject' box and messages should be annoymised wherever possible i.e. the use of a reference rather than individual names.

- Browsers are safely set up so that, for example, passwords are not saved and temporary internet and e-mail files are deleted on exit.

- Information sent by email will be safely stored and archived as well as being incorporated into patient records.

- There is an audit trail to show who did what and when.

- There are adequate fall back and fail-safe arrangements.

- Information is not saved or copied into any PC or media that is "outside the NHS".

- Emails no longer required should be archived/deleted from the system (Ref: NHS Records Management Code of Practice – Retention Schedules).

There are occasions when patients ask to correspond with the Trust via e-mail. This is not the Trust's preferred method and patients must be advised that any correspondence conducted via unencrypted e-mail is not secure. The Trust does have an encryption facility which can be used when sharing information via e-mail and patients should be encouraged to use this method. However, if a patient is not happy to use our encryption facility, preferring to use their own e-mail address, we must reiterate to them that the information is not secure and that the Trust cannot guarantee the security of their data. As long as the patient confirms an understanding of this fact and accepts responsibility for continuing to use unsecured e-mail, and such acceptance is recorded in the patient notes, it is acceptable to use this method of corresponding with the patient.

Seek advice from the Information Governance Team or IT services, with regards to encryption solutions, secure erasing methods, or restricted access rights to shared drives.

Please also read the Stockport NHS Foundation Trust IT Acceptable Use Policy for more guidance.

6.1.6 Phone:

- Information should not usually be provided over the telephone as the identity of the caller cannot always be verified.
- Always confirm the name, job title, department, and organisation of the person requesting the information.
- Confirm the reason for the information request.
- Take a contact number i.e. main switchboard (never a direct line or mobile telephone number).
- Call them back (always call the switchboard) to confirm the details, if necessary.
- Check whether the information can be provided; if in doubt tell the enquirer that you will call them back.
- Only provide information to the person who requested it, do not leave messages.
- Ensure that you record details of the information disclosed, your name, date and time of disclosure, the reason for the disclosure, and who authorised the disclosure. Also record the recipient's name, job title, organisation and telephone number.
- Ensure that you have a password protected voice mail in operation for any messages that you might receive.

6.1.7 Other Transportation Arrangements:

- Person identifiable information, including paper records, should only be taken off site when absolutely necessary and appropriately authorised, e.g. for community nursing staff and, secure document carriers should be used at all times. This includes attendance at Inquests. It is not permitted, in accordance with the Inquest Policy, to transport the full Inquest pack to the Inquest. Staff should carry with them ONLY their own statement.
- Where information is required (and appropriate) to be transported off site, in these circumstances, sensitive information should be transported out of sight (in a car boot); should never be left unattended and should NEVER be left in the car overnight. If information cannot be returned to base at the end of a shift, it should be removed from the car and stored overnight in the member of staff's house/apartment.
- Original hospital patient case notes should not be taken off-site under any circumstances.
- A record of what information you are taking off-site should always be documented, including why, where and to whom you are taking it.
- Information must be transported in a sealed/secure container.

- Never leave person identifiable information unattended.
- Ensure that all information is returned back to the site as soon as possible, and that any records are updated.
- Personal data should not be sent outside of the UK without seeking advice from the Information Governance Team.

6.2 Displaying Personal Information (for example on white-boards)

Boards containing patient information / person identifiable information should ideally be sited in areas that are **not** generally accessible by the public, e.g. staff offices. These rooms should be clearly marked 'staff only' and windows obscured appropriately.

With regard to patient identifiable information recorded on Ward Whiteboards, it is Trust policy that only initials are used (the exceptions are where there are two patients with the same surname when an initial can be used **by exception**, ED and Paediatrics who may use a first name and an age). This requirement relates also to the smaller side-room Whiteboards but does not apply to whiteboards above a patient's bed when the full name can be used.

If it is absolutely necessary (and this must be by exception) to pur clinical information onto a whiteboard, the information must be abbreviated or symbolised so that only health professionals can understand the information and not other members of staff (or other patients/patient relatives) that may come into the department.

If it is absolutely necessary to put clinical information onto a whiteboard, the information should be abbreviated or symbolised so only health professionals can understand the information and not other members of staff that may come into the department.

The use of personal information in patient areas should be carefully considered and a risk assessment undertaken by an appropriate manager.

6.3. Sharing Information with other Organisations

Person Identifiable Information must only be shared if:

- You have patient consent or
- If a law says you have to or
- It's in the public interest

Employees of the Trust authorised to disclose information to other organisations outside the NHS must seek assurance that these organisations have a designated safe haven point for receiving personal information.

The Trust must be assured that these organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirements:

- Data Protection Act 1998.
- Common Law Duty of Confidence.
- Confidentiality: NHS Code of Practice 2003.

A general Information sharing protocol and individual information sharing agreement must be put in place with NHS and local government information sharing partners and organisations where personal information is to be shared. A template information sharing protocol can be found at appendix (b).

A confidentiality agreement should be used with commercial third party suppliers of information systems and services, including support, maintenance or consultancy where the third party may have remote access or access to person identifiable or sensitive data on-site, or off-site.

All flows of information coming in and going out of the department should be risk assessed as appropriate and recorded by completing the information/data flow mapping form, which is to be returned to the I.G. Department. Advice should be sought from the Information Governance Team, as required.

6.4 Sharing Information Internally with 3rd Parties

There will be occasions where you may have to work with people employed by an external 3rd party on Trust premises, on the Trust's behalf, e.g. external consultants or contractors. The Data Protection principles and the guidance around duty of confidentiality still apply. Unless it is for the purpose of providing **direct healthcare**, no identifiable information can be shared. Any identifiers must be removed before the information is shared and any sharing must be done in a secure manner.

6.5 Anonymisation process

The Trust has adopted a policy of anonymisation rather than pseudonymisation, which would involve specialist software products.

The overall aims of anonymisation are to enable:

- The legal and secure use of patient data for secondary purposes by the NHS and other organisations involved in the commissioning and provision of NHS-commissioned care.

- NHS business is not using identifiable data in its non-direct care related work wherever possible.

All regular reports and ad-hoc requests for patient or activity level data will have all patient identifiable data removed and therefore be effectively anonymised.

6.6 Secure File Transfer (SFT)

The SFT is designed to replace physical media transfers (e.g. CDs, DVDs, memory sticks, USB pen drives, paper copy) and also to enable the transfer of large documents electronically (up to 1GB). It involves registering with the SFT service and uploading your information to the site. The recipients are then contacted to advise that information is on the site for them and they can then log into the site using the password you have provided them with. Information transfer using this method is secure.

Further information and guidance is available on the Information Governance & Security Microsite or by contacting the IG Department directly.

7. IMPLEMENTATION

7.1 The responsibility of implementing this document, including training and other needs that arise shall remain with the author. Line managers have the responsibility to cascade information on new and revised policies/procedures and other relevant documents to the staff for which they manage.

Line managers must ensure that departmental systems are in place to enable staff (including agency staff) to access relevant policies, procedures, guidelines and protocols and to remain up to date with the content of new and revised policies, procedures, guidelines and protocols.

7.2 This document has been compiled by the Information Governance Team in consultation with Governance Leads for each Business Group by means of the Information Governance & Security Group.

Once finalised, the document will be presented to the Performance & Finance Committee. The document will then be displayed on the Information Governance & Security microsite on the Trust's intranet and on the Trust's website. Managers and Governance leads should ensure the information is cascaded to all staff.

8. MONITORING

The Trust will regularly monitor and audit its Safe Haven & Information Sharing practices for compliance with this policy.

The audit will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to processes, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the policy is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of audits will be reported to the Information Governance & Security Group, Performance & Finance Committee and the Audit Committee, as appropriate.

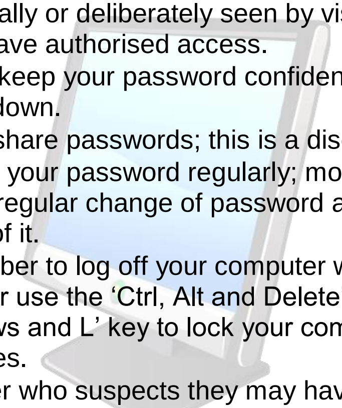
Monitoring Arrangements	Responsibility / Process / Frequency
Process for monitoring e.g. audit	- Internal Audit - Information Governance Toolkit - External Audit
Responsible individual/ group/ committee	Information Governance & Security Group
Frequency of monitoring	Annually
Responsible individual/ group/ committee for review of results	Information Governance & Security Group
Responsible individual/ group/ committee for development of action plan	Information Governance & Security Group
Responsible individual/ group/ committee for monitoring of action plan	Information Governance & Security Group

Mobile Computing - Laptops, Media, etc

- Personal and confidential information should not be taken off site unless absolutely necessary or without adequate protection.
- Mobile devices should be locked away in the building when not in use. Preferably behind a locked door and in a locked cupboard.
- Where it is absolutely necessary to store personal/confidential information on mobile devices:
  - ➢ Do not leave the device unattended
  - ➢ Remove confidential information as soon as possible; when no longer needed, using secure erasing methods.
  - ➢ Ensure that all devices you use are encrypted
  - ➢ Ensure regular housekeeping of all device files.

IT will advise on erasing and encryption solutions.

Computer

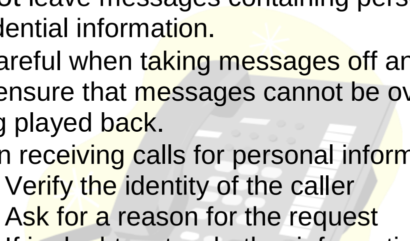


- Be careful where you site your computer screen: ensure any confidential or personal information cannot be accidentally or deliberately seen by visitors or staff who do not have authorised access.
- Always keep your password confidential and do not write it down.
- Do not share passwords; this is a disciplinary offence.
- Change your password regularly; most systems will force a regular change of password and designate the format of it.
- Remember to log off your computer when leaving the office, or use the 'Ctrl, Alt and Delete' keys' or the 'Windows and L' key to lock your computer for short absences.
- Any user who suspects they may have a computer virus must report it immediately to the IT helpdesk and log the issue as an incident in line with the incident management procedures.
- Any disk or CD coming into the organisation – no matter where it has come from – must be virus checked by the IT department before use.

Network Shared Drives

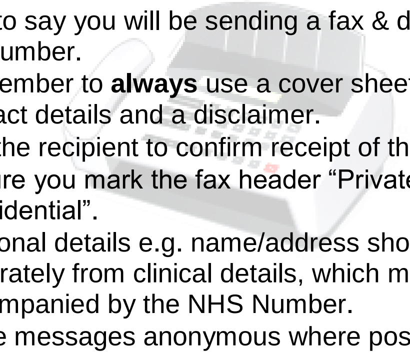
- Avoid storing confidential data on open shared drives.
- Ensure any files containing confidential/person identifiable data are restricted to the relevant members of staff.
- Use password protection on confidential/sensitive files and/or arrange for restricted access for specific users/groups, through the IT department.

Telephone



- Do not leave messages containing personal / confidential information.
- Be careful when taking messages off answer phones and ensure that messages cannot be overheard whilst being played back.
- When receiving calls for personal information:
  - ➢ Verify the identity of the caller
  - ➢ Ask for a reason for the request
  - ➢ If in doubt as to whether information should be disclosed tell the caller you will call them back. Take advice from your manager.
  - ➢ Call back to main switchboard or known and trusted numbers only – not direct lines you do not recognise or mobile telephones

Faxing

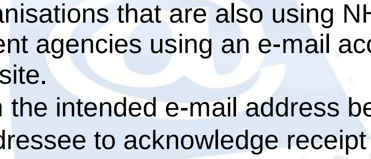


- Do not fax personal or confidential information unless it is **absolutely** necessary.
- If it is necessary, ensure that you fax the information to a Safe Haven/Secure fax location.
- Call to say you will be sending a fax & double check the fax number.
- Remember to **always** use a cover sheet, complete with contact details and a disclaimer.
- Ask the recipient to confirm receipt of the fax.
- Ensure you mark the fax header "Private and Confidential".
- Personal details e.g. name/address should be faxed separately from clinical details, which must be accompanied by the NHS Number.
- Make messages anonymous where possible.
- Program Fax machines to provide a transmission confirmation receipt or to periodically print a log of all calls made and received.

Database

- Ensure that any database, containing personal information, which is created, is in line with the Caldicott and Data Protection principles.
- Inform the Information Governance Team when new databases/system applications are created or introduced to your department/service.

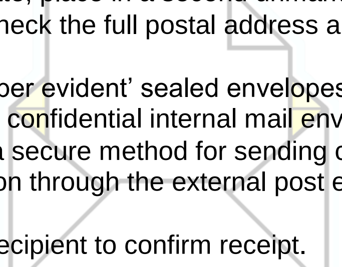
Email



Person Identifiable information should only be e-mailed if it is **absolutely** necessary and **encrypted** - where possible use NHS mail (@nhs.net) when sending to other NHS organisations that are also using NHS mail or other government agencies using an e-mail account listed on our microsite.

- Confirm the intended e-mail address beforehand.
- Ask addressee to acknowledge receipt of the e-mail
- Ensure no personal identifiable information is written in the subject box.
- Make messages anonymous where possible. i.e. use a reference rather than a name.

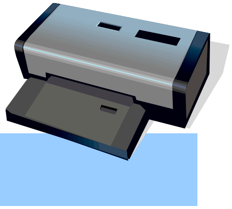
Post



- Ensure envelopes are marked "Private and Confidential – to be opened by addressee only" and, where appropriate, place in a second unmarked envelope.
- Double check the full postal address and name of the recipient.
- Use 'tamper evident' sealed envelopes for external post or sealed confidential internal mail envelopes.
- Choose a secure method for sending confidential information through the external post e.g. recorded delivery.
- Ask the recipient to confirm receipt.
- Ensure that incoming confidential post is handled appropriately and that outgoing mail is sent to a safe place.
- Confirm receipt of any confidential information received.
- Ensure all mail goes through the post room for franking.

Printer

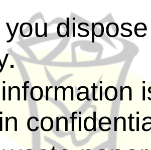
- Avoid printing confidential/personal information to central printers, where it may be left unattended.
- Keep the number of copies to a minimum.



Photocopying

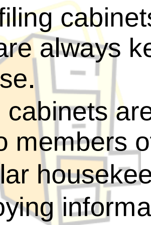
- Do not make excessive copies of confidential information.
- Regularly check /update your distribution list to ensure copies are not sent to staff who have left or moved to another service.

Bin



- Be sure that you dispose of confidential information appropriately.
- All personal information is confidential and must be disposed of in confidential waste bags for shredding.
- Confidential waste paper must not be used as scrap paper for messages, notes etc.

Filing Cabinet

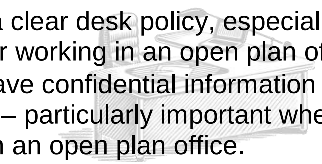


- Ensure that filing cabinets containing confidential information are always kept locked when not in immediate use.
- Ensure filing cabinets are not sited in areas which are accessible to members of the public/visitors.
- Ensure regular housekeeping of your files.
- When destroying information ensure you comply with NHS retention guidelines.

Office

- Remember to lock and secure the office when it is unattended and at the end of the day.
- Whenever possible escort visitors at all times on site.
- Remember to wear your identity badge.

Desk



- Operate a clear desk policy, especially when hot desking or working in an open plan office.
- Do not leave confidential information unattended or out overnight – particularly important when hot desking or working in an open plan office.
- Lock confidential information away, where possible.

Person

- Ensure you hold confidential conversations in an appropriate place. Inappropriate places include corridors, open plan offices, and at the photocopier!
- Gain the patient's consent before sharing their personal information with relatives.

For further information and advice, please contact:

The Information Governance & Security department on:

0161 419 5295 / 4364

E-mail:
Information.Governance@stockport.nhs.uk

Or Visit the:
Information Governance & Security Microsite on the Trust Intranet

This leaflet is available in large print format on request.

Ref: IG01
September 2011 **Version 1.4**

Stockport
NHS Foundation Trust

Guidance for Safe Havens & Sharing Personal Information

It's your responsibility…

Compliance with Data Protection, Caldicott and Information Security Best Practice

'Confidentiality, Security and Accuracy'

Stockport NHS Foundation Trust

Appendix (b)

Information Sharing Protocol

Between: ________________________________ **(the "Recipient")**

And: **Stockport NHS Foundation Trust (the "Trust")**

The Recipient has a legitimate interest in accessing and using certain personal information held by the Trust. This Information Sharing Protocol sets out the basis upon which the Trust will share personal data with the Recipient and the steps that both parties will take to ensure that personal data is protected adequately at all times.

The first part of this Information Sharing Protocol sets out general principles with which both parties must comply at all times. Appendix 1 describes the categories of data that will be shared with the Recipient and the purpose(s) for which the Recipient is permitted to use each category of data. Appendix 2 sets out the security measures that the parties shall put in place to protect the data. Appendix 3 sets out details of the key contacts of each party, who have overall responsibility for information governance in connection with the information sharing arrangement.

From time to time the parties may agree additional protocols to govern specific aspects of the data sharing (for example detailed operational procedures for sharing data). Such additional protocols must be agreed in writing by authorised representatives of both parties and will be supplemental to this Information Sharing Protocol.

For the purposes of this Information Sharing Protocol, the terms "personal data", "data subject" and "data controller" shall have the same meaning given to those terms in the Data Protection Act 1998.

General Principles

1. Each party recognises that the other party is a data controller in its own right. Both organisations agree to comply with the various principles set out in this Information Sharing Protocol and their respective obligations under the Data Protection Act 1998.

2. Each party shall appoint a responsible officer who will be responsible for ensuring the protection of personal information that is shared in accordance with this Information Sharing Protocol (each a "**Responsible Officer**"). The Responsible Officer must have appropriate training and experience to fulfil the role (e.g. Caldicott Guardian or senior manager responsible for data protection). Details of the Responsible Officers appointed by the parties at the date of signing this Information Sharing Protocol are set out in Appendix 3. The parties may change their appointed Responsible Officer by notice in writing to the other party.

3. The categories of data that the Trust will share with the Recipient are set out in Appendix 1. The Recipient is solely permitted to use the data provided by the Trust for the relevant purpose(s) specified in Appendix 1. From time to time the parties may amend the categories of data being shared and the purposes for which data may be used by the Recipient. Any such changes must be approved in writing by the Responsible Officers prior to any data transfer occurring and an updated Appendix A shall be prepared to reflect the agreed changes.

4. The Trust shall use reasonable endeavours to provide the personal data to the Recipient in the format specified in Appendix 1 at the frequency specified in Appendix 1. The Trust does not give any warranty as to the accuracy, completeness or fitness for purpose of any data provided to the Recipient and the Recipient shall be responsible for determining whether the data provided by the Trust is suitable for use by the Recipient for the permitted purpose. The Trust shall not be responsible

for any losses or damage suffered by the Recipient as a result of use of any data provided by the Trust or otherwise arising in connection with the information sharing arrangements governed by this Information Sharing Protocol.

5. Each party shall ensure that it has in place appropriate procedures and measures to ensure compliance with the Data Protection Act 1998, the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("the Data Protection Legislation"), Caldicott Report, BS ISO/IEC 27000 Series of Information Security Standards and national guidance and rules around holding and destroying health/social services records and other relevant legislation.

6. Both parties shall take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against the accidental loss or destruction of, or damage to, personal data to ensure compliance with the seventh data protection principle including, but not limited to, the security measures set out in Appendix 2.

7. The Recipient shall promptly comply with any request from the Trust to amend or delete any personal data that has been provided by the Trust.

8. At the end of the retention period specified in Appendix 1, the Recipient shall delete or destroy the personal data securely in accordance with the requirements set out in Appendix 2.

9. If the Recipient receives any complaint, notice or communication which relates directly or indirectly to the processing of the personal data provided by the Trust or to the Recipient's compliance with the Data Protection Legislation, it shall immediately notify the Trust and it shall provide the Trust with full co-operation and assistance in relation to any such complaint, notice or communication.

10. The Recipient shall not transfer the personal data provided by the Trust to any third party or outside the European Economic Area without the prior written consent of the Trust.

11. Each party shall respect the rights of data subjects under the Data Protection Legislation and shall provide reasonable co-operation and assistance to the other party to ensure that rights may be exercised effectively by data subjects. It is anticipated that each party shall be responsible for responding to requests that the relevant party receives from data subjects. To the extent that a request is received which relates to the data sharing arrangements governed by this Information Sharing Protocol, the parties shall consult with one another and agree which party is best placed to respond to the request.

12. Each party is committed to reviewing practice with the aim of ensuring all exchanges of personal information meet legal and Caldicott standards. The parties shall regularly review this Information Sharing Protocol and the practices and procedures that each party has in place to ensure that information sharing is carried out in accordance with all applicable laws and regulatory guidance. The parties shall carry out reviews not less than once in each 12 month period. Reviews shall include:

    a. consideration of whether it is still necessary to share each category of data listed in Appendix 1;
    b. a review of all data listed in Appendix A to ensure that only the minimum necessary level of data is being shared;
    c. a review of the quality and accuracy of data and ways in which quality and accuracy may be improved;
    d. a review of whether the retention periods specified in Appendix 1 are appropriate;
    e. consideration of whether the security measures in place to protect personal data are adequate and whether security measures can be improved;
    f. the level of staff awareness in relation to data protection requirements and the obligations placed on the parties under this Information Sharing Protocol and whether additional staff training needs to take place;
    g. the processes that the parties have in place to ensure that individuals can exercise their rights effectively in relation to the information sharing arrangements.

13. Each party is committed to ensuring staff are informed of the confidential nature of the personal data, are appropriately trained in data protection/Caldicott procedures and have been issued with practical guidelines on the transfer of personal information. In the case of the Recipient, access to the personal data shall be restricted to those staff who require it in order to achieve the permitted purposes set out in Appendix 1.

14. Either party may terminate this Information Sharing Protocol at any time upon given written notice to the other party. Upon termination, the Recipient shall delete or destroy all personal data provided by the Trust under this Information Sharing Protocol in accordance with the requirements set out in Appendix 2.

15. The Recipient shall indemnify the Trust and keep indemnified the Trust from and against all costs, expenses (including, but not limited to, legal and other professional fees and expenses) losses, damages and other liabilities (of whatever nature, whether contractual, tortious or otherwise) suffered or incurred by the Trust and arising out of or in connection with any breach of this Information Sharing Protocol by the Recipient, any activities of the Recipient in connection with the data provided by the Trust pursuant to this Information Sharing Protocol and any claims, actions or demands made against the Trust by any third party as a result of any breach or alleged breach of this Information Sharing Protocol by the Recipient.

Signed on behalf of the Recipient:

______________________________ ________________________ ____________

Signature Print name Date
Caldicott Guardian/authorised officer

Signed on behalf of the Trust:

______________________________ ________________________ ____________

Signature Print name Date
Caldicott Guardian/authorised officer

APPENDIX 1 – PERMITTED PURPOSES AND DATA ITEMS

Information flows from the Trust to the Recipient

Flow number/ code	Flow name	Sender Department and/or borough if not Trust wide	Recipient, department or person?	Purpose	Data Items*	Format/ applicable data standards	Frequency of data sharing	Retention period	Justified by and date

*See the table below for an explanation of different categories of data items. In each case a precise description of the categories of data to be provided must be given.

Definition of Data Items

No.	**Data Item**	**Definition**
1	Personal	Name Date of birth Next of kin Personal circumstances Financial information Physical description Gender NHS Number
2	Personal/ Sensitive	Racial/ethnic origin Religion Trade Union membership Court Proceedings Criminal convictions Political opinions
3	Clinical (Sensitive)	Information relating to physical or mental health or condition
4	Demographic	Address Postcode Telephone number Location description Directions
5	Other	Environmental Social Health Professional
6	Confirmed and/or unconfirmed risk	Risk to self Risk to children Risk to staff/professionals Risk to others

APPENDIX 2 – DATA SECURITY MEASURES

[*Include details of appropriate security measures relating to the information sharing that the parties must put in place to ensure that data is kept securely*.]

Information Governance Training

All individual recipients must have undertaken appropriate Data Protection and confidentiality training.

IT System Access

All systems access must be authorised by an appropriate manager at the Trust and all individuals requiring access to the Trust's information systems will be required to undertake systems specific training prior to any access being granted.

Transmission of data

The parties shall transmit data in accordance with NHS data encryption and/or physical security standards, specifically the following procedures:

[*Insert specific requirement for transmitting data*]

Storage of data

The Recipient shall ensure that all data received from the Trust shall be stored and processed in accordance with NHS data encryption standards and the following security procedures:

[*Insert specific details*]

Retention, deletion and destruction of data

The Recipient shall comply with the following requirements when archiving/deleting/destroying data provided by the Trust pursuant to this Information Sharing Protocol:

DH NHS Records Management Code of Practice requirements and;
[*Insert specific standards for deleting and destroying data*]

Statement of personal responsibility

All of the recipient's employees will be required to agree to and sign a statement of personal responsibility (Appendix 4) prior to being given access to any of the Trust's information.

APPENDIX 3 – RESPONSIBLE OFFICERS

Trust

Name: Khaja Hussain
Role: Assistant Director of Information Governance & Security
Telephone: 0161 419 5295
Email: Khaja.hussain@stockport.nhs.uk
Address: Stepping Hill Hospital, Poplar Grove, Stockport, Cheshire. SK2 7JE

Recipient

Name:
Role:
Telephone:
Email:
Address:

,,mmmm

APPENDIX 4 – AGREEMENT OUTLINING PERSONAL RESPONSIBILITY CONCERNING SECURITY AND CONFIDENTIALITY OF INFORMATION:

In connection with services provided by your employer to the Stockport NHS Foundation Trust (the "Trust") you may acquire or have access to confidential information (including personal information) which must not be disclosed to any other person unless in pursuit of your duties as detailed in the Information Sharing Protocol with the Trust.

In consideration of being given access to such confidential information, you hereby agree that such confidential information shall be treated by you as confidential and you agree as follows:

1. In this agreement "Confidential Information" shall mean information of whatever kind (whether commercial, technical, financial, operational or otherwise, whether communicated verbally, in writing or in any other form, and whether or not expressly stated to be confidential) provided or made available to you by or on behalf of the Trust including (but not limited to):
    a. the existence or contents of this agreement;
    b. information relating to the operation, business, employees, patients or suppliers of the Trust;
    c. any other information generated or acquired by you in relation to the Trust; and
    d. any modification (whether authorised or otherwise) made to any of the information mentioned in this paragraph 1 by you or any person to whom you have disclosed any of that information.
2. You will safeguard the Confidential Information and treat it with the strictest confidence and will not without the prior written consent of the Trust disclose, reveal, report, publish or transfer any Confidential Information to any third party.
3. You will divulge the Confidential Information only to those of your fellow employees who are directly concerned with the provision of services to the Trust and who have a legitimate need to know or use such information or documents for the purposes of fulfilling their responsibilities and who have prior to such disclosure entered into an agreement with the Trust in the same form as this agreement or in such other form as may be approved by the Trust.
4. You will ensure that any such employees to whom you divulge any Confidential Information are aware that the same is confidential to the Trust.
5. You will not use the Confidential Information for any purpose other than for the fulfilment of your duties in connection with the provision of services to the Trust.
6. All papers furnished to you by the Trust (whether directly or through your employer) or generated or acquired by you will be returned or otherwise disposed of as the Trust may from time to time direct.
7. You will not make any copies (whether in physical or electronic form) of any Confidential Information.
8. The obligations set out in this agreement shall continue in full force and effect notwithstanding the completion of the services, and/or the termination of your involvement with the provision of the services.

If you are found to have used any information you have seen or heard whilst working with the Trust in breach of this agreement you and your employer may face legal action.

<u>Statement of Acceptance:</u>

I understand that I am bound by a duty of confidentiality and agree to adhere to the conditions set out above.

Name of employer:	
Contact details (Dept./Tel):	
Print Name / Job Title:	
Signature:	
Date:	

Stockport NHS
NHS Foundation Trust

Appendix 1

Office Use Only

Submission Date:	**13/4/17**
Approved By:	
Full EIA needed:	**Yes/No**

Equality Impact Assessment – Policies, SOP's and Services not undergoing re-design

1	**Name of the Policy/SOP/Service**	Information Sharing & Transfer of Records Policy	
2	**Department/Business Group**	Information Governance – IM&T	
3	**Details of the Person responsible for the EIA**	**Name:** **Job Title:** **Contact Details:**	Jean Lehnert I.G. Co-ordinator 0161 419 4364
4	**What are the main aims and objectives of the Policy/SOP/Service?**	To provide guidance for staff in order to maintain and uphold the Trusts information governance requirements	

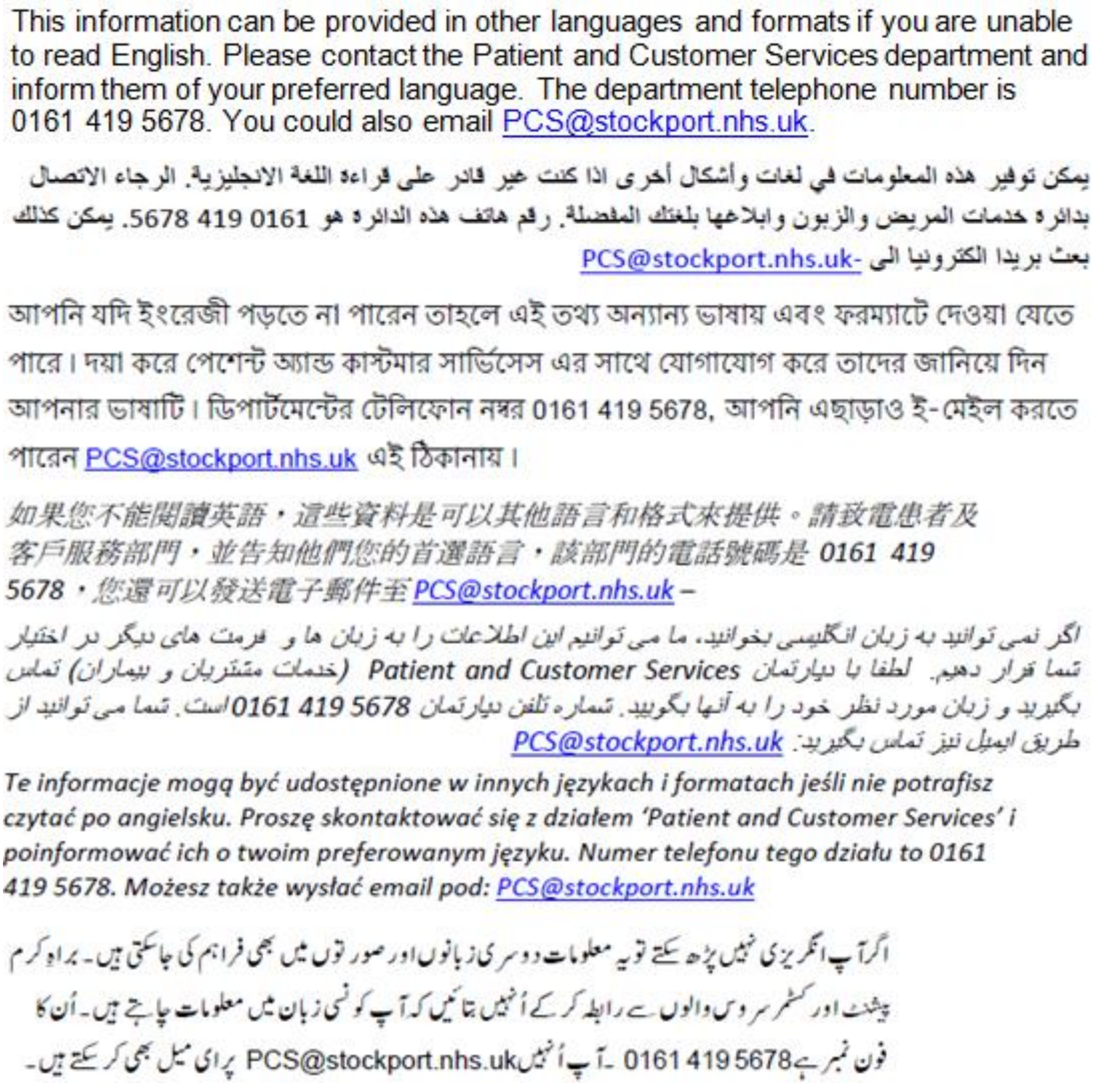
or the following question, please use the EIA Guidance document for reference:

5	**A) IMPACT** **Is the policy/SOP/Service likely to have a <u>differential</u> impact on any of the protected characteristics? If so, is this impact likely to be positive or negative?** **Consider:** • Does the policy/SOP apply to all or does it exclude individuals with a particular protected characteristic e.g. females, older people etc.? • What does existing evidence show? E.g. consultation from different groups, demographic data, questionnaires, equality monitoring data, analysis of complaints. Are individuals from one particular group accessing the policy /SOP /Service more/less than expected?	**B) MITIGATION** **Can any potential negative impact be justified? If not, how will you mitigate any negative impacts?** ✓ Think about reasonable adjustment and/or positive action ✓ Consider how you would measure and monitor the impact going forward e.g. equality monitoring data, analysis of complaints. ✓ Assign a responsible lead. ✓ Designate a timescale to monitor the impacts. ✓ Re-visit after the designated time period to check for improvement.	**Lead**
Age	This Policy concerns itself with information as a generic term – it does not reference specific details relating to any individual.		
Carers / People with caring responsibilities	This Policy concerns itself with information as a generic term – it does not reference specific details relating to any individual.		
Disability	This Policy concerns itself with information as a generic term – it does not reference specific details relating to any individual.		
Race / Ethnicity	This Policy concerns itself with information as a generic term – it does not reference specific details relating to any individual.		

Gender	This Policy concerns itself with information as a generic term – it does not reference specific details relating to any individual.		
Gender Reassignment	This Policy concerns itself with information as a generic term – it does not reference specific details relating to any individual.		
Marriage & Civil Partnership	This Policy concerns itself with information as a generic term – it does not reference specific details relating to any individual.		
Pregnancy & Maternity	This Policy concerns itself with information as a generic term – it does not reference specific details relating to any individual.		
Religion & Belief	This Policy concerns itself with information as a generic term – it does not reference specific details relating to any individual.		
Sexual Orientation	This Policy concerns itself with information as a generic term – it does not reference specific details relating to any individual.		
General Comments across all equality strands	This Policy concerns itself with information as a generic term – it does not reference specific details relating to any individual.		

EIA Sign-Off	**Your completed EIA should be sent to Sue Clark , Equality and Diversity Manager for approval and publication:** Susan.clark@stockport.nhs.uk **0161 419 4784**

If you would like this policy in a different format, for example, in large print, or on audiotape, or for people with learning disabilities, please contact:
Patient and Customer Services, Poplar Suite, Stepping Hill Hospital. Tel: 0161 419 5678.
Email: PCS@stockport.nhs.uk.



This information can be provided in other languages and formats if you are unable to read English. Please contact the Patient and Customer Services department and inform them of your preferred language. The department telephone number is 0161 419 5678. You could also email PCS@stockport.nhs.uk.

يمكن توفير هذه المعلومات في لغات وأشكال أخرى اذا كنت غير قادر على قراءه اللغة الانجليزية. الرجاء الاتصال
بدائره خدمات المريض والزبون وابلاغها بلغتك المفضلة. رقم هاتف هذه الدائره هو 0161 419 5678. يمكن كذلك
بعث بريدا الكترونيا الى -PCS@stockport.nhs.uk

আপনি যদি ইংরেজী পড়তে না পারেন তাহলে এই তথ্য অন্যান্য ভাষায় এবং ফরম্যাটে দেওয়া যেতে পারে। দয়া করে পেশেন্ট অ্যান্ড কাস্টমার সার্ভিসেস এর সাথে যোগাযোগ করে তাদের জানিয়ে দিন আপনার ভাষাটি। ডিপার্টমেন্টের টেলিফোন নম্বর 0161 419 5678, আপনি এছাড়াও ই-মেইল করতে পারেন PCS@stockport.nhs.uk এই ঠিকানায়।

如果您不能閱讀英語・這些資料是可以其他語言和格式來提供。請致電患者及客戶服務部門・並告知他們您的首選語言・該部門的電話號碼是 0161 419 5678・您還可以發送電子郵件至 PCS@stockport.nhs.uk –

اگر نمی توانید به زبان انگلیسی بخوانید، ما می توانیم این اطلاعات را به زبان ها و فرمت های دیگر در اختیار
شما قرار دهیم. لطفا با دپارتمان Patient and Customer Services (خدمات مشتریان و بیماران) تماس
بگیرید و زبان مورد نظر خود را به آنها بگویید. شماره تلفن دپارتمان 0161 419 5678است. شما می توانید از
طریق ایمیل نیز تماس بگیرید: PCS@stockport.nhs.uk

Te informacje mogą być udostępnione w innych językach i formatach jeśli nie potrafisz czytać po angielsku. Proszę skontaktować się z działem 'Patient and Customer Services' i poinformować ich o twoim preferowanym języku. Numer telefonu tego działu to 0161 419 5678. Możesz także wysłać email pod: PCS@stockport.nhs.uk

اگر آپ انگریزی نہیں پڑھ سکتے تو یہ معلومات دوسری زبانوں اور صورتوں میں بھی فراہم کی جا سکتی ہیں۔ براہ کرم
پیشنٹ اور کسٹمر سروس والوں سے رابطہ کر کے اُنہیں بتائیں کہ آپ کونسی زبان میں معلومات چاہتے ہیں۔ اُن کا
فون نمبر ہے0161 419 5678 ۔ آپ اُنہیںPCS@stockport.nhs.uk پر ای میل بھی کر سکتے ہیں۔

Appendix 1

Office Use Only

Submission Date:	
Approved By:	
Full EIA needed:	**Yes/No**

Equality Impact Assessment – Policies, SOP's and Services not undergoing re-design

1	**Name of the Policy/SOP/Service**	Information Sharing & Transfer of Records Policy	
2	**Department/Business Group**	Information Governance/IM&T	
3	**Details of the Person responsible for the EIA**	**Name:** **Job Title:** **Contact Details:**	Jean Lehnert I.G. Co-ordinator X 4364
4	**What are the main aims and objectives of the Policy/SOP/Service?**	To ensure that identifiable information is handled securely and appropriately	

For the following question, please use the EIA Guidance document for reference:

5	**A) IMPACT** **Is the policy/SOP/Service likely to have a <u>differential</u> impact on any of the protected characteristics? If so, is this impact likely to be positive or negative?** **Consider:** • Does the policy/SOP apply to all or does it exclude individuals with a particular protected characteristic e.g. females, older people etc.? • What does existing evidence show? E.g. consultation from different groups, demographic data, questionnaires, equality monitoring data, analysis of complaints. Are individuals from one particular group accessing the policy /SOP /Service more/less than expected?	**B) MITIGATION** **Can any potential negative impact be justified? If not, how will you mitigate any negative impacts?** ✓ Think about reasonable adjustment and/or positive action ✓ Consider how you would measure and monitor the impact going forward e.g. equality monitoring data, analysis of complaints. ✓ Assign a responsible lead. ✓ Designate a timescale to monitor the impacts. ✓ Re-visit after the designated time period to check for improvement.	**Lead**
Age	The policy does not discriminate on the basis of age – the policy concerns itself with handling information according to legal requirements, over which the Trust has no control.		
Carers / People with caring responsibilities	The policy does not discriminate against carers/people with caring responsibilities – the policy concerns itself with handling information according to legal requirements, over which the Trust has no control.		
Disability	The policy does not discriminate on the basis of disability – the policy concerns itself with handling information according to legal requirements, over which the Trust has no control.		

Race / Ethnicity	The policy does not discriminate on the basis of race/ethnicity – the policy concerns itself with handling information according to legal requirements, over which the Trust has no control.		
Gender	The policy does not discriminate on the basis of gender – the policy concerns itself with handling information according to legal requirements, over which the Trust has no control.		
Gender Reassignment	The policy does not discriminate against those subject who have undergone/are undergoing gender re-assigment – the policy concerns itself with handling information according to legal requirements, over which the Trust has no control.		
Marriage & Civil Partnership	The policy does not discriminate on the basis of marital/civil partnership status – the policy concerns itself with handling information according to legal requirements, over which the Trust has no control.		
Pregnancy & Maternity	The policy does not discriminate on the basis of Pregnance/Maternity status – the policy concerns itself with handling information according to legal requirements, over which the Trust has no control.		
Religion & Belief	The policy does not discriminate on the basis of religion and/or belief – the policy concerns itself with handling information according to legal requirements, over which the Trust has no control.		
Sexual Orientation	The policy does not discriminate on the basis of sexual orientation – the policy concerns itself with handling information according to legal requirements, over which the Trust has no control.		
General Comments across all equality strands	This policy does not concern itself with individual aspects/characteristics of Trust patient and/or staff and/or carers. The content seeks to advise/guide staff on their responsibilities when handling identifiable information and is written in accordance with UK legislation – over which the trust has no control		

EIA Sign-Off	**Your completed EIA should be sent to Sue Clark , Equality and Diversity Manager for approval and publication:** safina.nadeem@stockport.nhs.uk **0161 419 4784**