Leeds and York Partnership NHS
NHS Foundation Trust

Safe Haven Guidance

Date effective from:	01/02/2016
Review date:	01/02/2019
Version number:	2.0

See Document Summary Sheet for full details

CONTENTS

DOCUMENT SUMMARY SHEET

ALL sections of this form must be completed. Those marked with * will be used as search information on Staffnet.

Document title*:	Safe Haven Guidance
Document Reference Number *	IG-0009
Member of the Executive Team Responsible* (Title):	Chief Financial Officer (as SIRO)
Document author* (Name and title):	Carl Starbuck Information & Knowledge Manager
Approved by (Committee/Group):	Information Governance Group
Date approved:	20/01/2016
Ratified by (Committee/Board):	Information Governance Group
Date ratified:	20/01/2016
Review date:	01/02/2019
Frequency of review:	Every 3 years
Responsible for the review:	Information & Knowledge Manager
Target audience: (List, by title, the people this procedural document is essential for)	Staff who send or receive personal, sensitive, or otherwise confidential information
Responsible for dissemination:	Information & Knowledge Manager

DOCUMENT AMENDMENT SHEET

Please record what changes you have made to the procedural document since the last version.

This is a summary of changes to the document and is designed to show people exactly what has changed. The version number recorded below should correspond to the ratified version number shown on the Document Summary Sheet.

Version	Amendment	Reason
0.1	1st draft of new procedural document	Replacing old fax-only policy with a wider Safe Haven procedural document, encompassing all aspects of data movement.
0.2	Correction of MG7 group name.	After approval by MG7, 18/04/2011
1.0	Ratified	Ratified by Executive Team, 10/05/2011
1.1	Review and update	Document at review date. Content update aligned to ICO IRR review (October 2015)
2.0	Approved & Ratified	Approved and ratified as guidance by IG Group, 20/01/2016

PART A

1 EXECUTIVE SUMMARY

The “Safe Haven” concept is about the locations and transport methods for personal, sensitive and otherwise confidential data being appropriately secure. Given the proliferation of transport mechanisms, the Trust approach to Safe Havens must encompass a wide array of communications methods. With the advent of increased access to mobile working solutions and remote access to Trust systems, it is important to focus not solely on systems and technology, but for all of us to act as a “Personal Safe Haven” whenever we handle personal, sensitive and otherwise confidential information. Essentially, our methods and personal practices must make each of us a “safe pair of hands” for the confidential information we use.

2 THE PROCEDURE

2.1 Flow Chart of Procedure

Not applicable for this guidance document.

2.2 A Scalable Approach to Confidential Communications

The Trust accepts that there is a wealth of routine communication, by paper and electronic means, which happens during the normal course of clinical and business operations. Each individual should communicate and behave in a manner which is both appropriate and proportional in security to the content of the material they are handling. We are all responsible for the decisions we make regarding the confidentiality of our data and its storage and transfer. Further guidance should always be sought if you are unsure.

2.3 E-Mail

The Trust uses the NHS.net e-mail service. This service is endorsed for the communication of personal and sensitive information by the Health & Social Care Information Centre, the British Medical Association, the Royal College of Nursing and the Chartered Society of Physiotherapists.

NHS.net e-mail is automatically encrypted in transit, therefore any e-mail sent from one NHS.net mail account to another (e.g. xxx@nhs.net to yyy@nhs.net) is secure.

NHS.net e-mail is hosted on the N3 network and is part of the wider public sector Government Secure Intranet (GSi). This means that we can also be assured that e-mail is encrypted when delivered to any of the following e-mail domains:-

Secure email domains in Central Government:

- *.gsi.gov.uk
- *.gse.gov.uk
- *.gsx.gov.uk

The Police National Network/Criminal Justice Services secure email domains:

- *.police.uk
- *.pnn.police.uk
- *.scn.gov.uk
- *.cjsm.net

Secure email domains in Local Government/Social Services:

- *.gcsx.gov.uk

E-mail sent to / from NHS.net addresses and e-mail addresses ending in the above will be secure in transit, giving us secure communications with various public sector partner organisations.

NHS.net mail should not be confused with NHS e-mail addresses ending with NHS.UK. An example of this is the old Trust e-mail accounts, formatted xxx@leedspft.nhs.uk – these addresses are not secure when sending from NHS.net accounts.

When sending outside the GSi network, personal, sensitive and otherwise confidential information must be removed from the subject line and body text of the document and alternate methods of encryption must be used. Appendices A & B detail alternative approaches to encryption.

2.4 Fax

With the advent of secure e-mail within the Trust and beyond, fax transfer is now seen as an outdated technology. However we recognise that with some partner organisations this legacy technology remains in use.

Some practical steps are required to ensure that the use of fax does not compromise security, as follows:-

Sending:-

- Personal, sensitive and confidential information should only be sent to a fax machine where the sender is confident that safeguards are in place to ensure its security. It is advisable to make contact ahead of sending any confidential information by fax to confirm the number and security of the receiving fax.
- Fax header sheets should be used which identify a named sender and recipient and have “Private and Confidential” marking.
- Speed dials should be used with caution and checked regularly. Although correctly programmed speed dials may enhance the likelihood that faxes are delivered to the correct recipient, an incorrectly selected speed dial will result in the fax being delivered to an incorrect fax endpoint.
- When dialling manually or via speed dial, the onus is on the sender to verify the fax number.

Receiving:-

- The fax machine’s location is physically secure. Access to the fax machine is such that only those satisfying the “need to know” principle have access to it. This is usually via the fax being sited in a secure office or cupboard.
- The location is out of public view. It will not be visible from the public side of a reception area, or window without obscured glass.
- If sited in an office which is unmanned out of hours, fax printing is prevented during unmanned periods. This may be achieved by either removing the paper or putting the fax in “memory receive” or similar offline mode.

2.5 Internal Mail

Internal mail containing personal, sensitive or otherwise confidential information must be sent in a securely sealed envelope or container, marked “Private and Confidential”. End-to-end delivery assurance can be achieved by the sender logging the outgoing data and confirming safe delivery with the recipient by phone or e-mail. Personal, sensitive or otherwise confidential information should be sent to a named recipient who is aware of and expecting the transfer whenever practicable.

All mail should be received and opened on the “staff side” of any site which has service user / non-staff access.

2.6 External Mail – Non-Traceable 1st / 2nd Class Mail & Parcel Post

External mail containing personal, sensitive or otherwise confidential information must be sent in a securely sealed envelope or container, marked “Private and Confidential”. End-to-end delivery assurance can be achieved by the sender logging the outgoing data and confirming safe delivery with the recipient by phone or e-mail. Personal, sensitive or otherwise confidential information should be sent to a named recipient who is aware of and expecting the transfer whenever practicable.

All mail should be received and opened on the “staff side” of any site which has service user / non-staff access.

It should be noted that point 2.2 is relevant to both internal and external mail transfers. Expectations of security should be scaled to the application. For example, we would not expect every letter sent to a service user, GP or other endpoint which contains correspondence about a single service user to be secured beyond the use of ordinary 1st / 2nd class mail. To do so would exceed the expectations of the process and the recipient. However should we be moving volumes of information (e.g. ‘bulk’ data transfers relating to several subjects), or when sending highly sensitive data, we would consider enhancing the security using traceable methods. See section 2.7 below.

2.7 Traceable Mail Services and Courier Deliveries

Personal, sensitive or otherwise confidential information may be sent by commercial courier method to enhance security. This includes Royal Mail “Special Delivery” and similar courier services. End-to-end delivery assurance can be achieved by the sender logging the outgoing data and confirming safe delivery with the recipient by phone or e-mail in addition to tracking and tracing the delivery. Personal, sensitive or confidential information should be sent to a named recipient who is aware of and expecting the transfer whenever practicable.

To be fit for purpose, the delivery service should allow for full tracking / tracing along the delivery route to delivery endpoint. The Royal Mail “Signed For” service is NOT traceable along the delivery route.

2.8 Personal Delivery (By Hand)

Staff may elect to deliver personal, sensitive or confidential information by hand. Whilst this may give the person delivering the information assurance that the delivery has taken place, it should be noted that this may result in a lack of audit trail for the transfer. By hand deliveries should therefore be used where formal proof of delivery is either not necessary or achieved by an agreed method, e.g. signature on delivery.

2.9 Portable Digital Media / Document Encryption

Since the HMRC Child Benefit data loss in October 2007, the security of personal, sensitive or otherwise confidential information moved on portable digital media has received heightened scrutiny. Any personal, sensitive or otherwise confidential information moved on portable digital media must:-

- Be encrypted to an appropriate standard and / or
- Protected in transit using a secure, traceable delivery mechanism

Ideally, both of the above measures should be employed.

The Trust has procured a supply of hardware encrypted USB memory sticks. These sticks operate AES 256 bit encryption and are authorised for the transport of personal, sensitive or otherwise confidential information.

Microsoft Office supports file-level encryption, allowing users to encrypt Word documents and Excel spreadsheets for communication by otherwise unencrypted e-mail or portable media. Appendix A has guidance on using encryption in MS-Office 2010.

2.10 The “New Safe Haven” – Secondary Use Protection

The Trust has developed the “New Safe Haven” concept as part of the Pseudonymisation Implementation Project. It is a privacy-enhancing working arrangement designed to increase security of patient-identifiable data when used for secondary purposes.

Pseudonymisation is a process by which an identifier is created using an electronic algorithm that can only be interpreted by having access to the pseudonymisation key. The "New Safe Haven" has the following characteristics:-

- Data will be pseudonymised before being accessed or transferred for secondary purposes
- Staff working within the "New Safe Haven" will be able to decipher and thus identify the subjects of pseudonymised data.
- Patient identifiable (i.e. non-pseudonymised) data can be exchanged between the "New Safe Havens" of partner organisations.
- The "New Safe Haven" will be a virtual working group, with members identified and permitted by role.

Pseudonymisation can only function when sender and recipient are prepared to work with pseudonymised identifiers. Although our Trust has a fully implemented pseudonymisation solution, we may work with strategic partners who have not implemented it. In those cases, we must communicate patient level data using other methods outlined above so we maintain the security of information and honour our obligations under the seventh principle of the Data Protection Act (1998) and the Caldicott Principles.

In the absence of "New Safe Haven" arrangements at a partner organisation, a combination of both document-level encryption and / or secure GSi e-mail is considered appropriate protection.

2.11 Personal Safe Haven Working

The most important aspect of information security is the 'Human Element'. It is not sufficient to simply consider systems and devices as the entire scope of the Safe Haven concept, particularly with the advent of mobile / remote access and agile working arrangements. All staff must adopt working practices so that they can be considered a "Personal Safe Haven" – essentially a safe pair of hands for personal, sensitive or otherwise confidential information.

Basic and common sense steps will help us all to meet this important obligation:-

- Maintain an awareness of your surroundings and the threats to information security in your immediate vicinity.
- Ensure PCs are locked or switched off when not in use.
- Make sure that laptop / PC screens are not inappropriately viewed by 3rd parties, particularly when working remotely.
- Ensure information is not visible or accessible to inappropriate people.

- Clear desks and other workspaces of information when leaving a workstation.
- Ensure that information transferred between locations arrives intact, without total or partial loss en-route.
- Store information in the boot of a car when in transit.
- Remove personal, sensitive or confidential information from any vehicle on arrival at your work base, home, or final location.
- Only take & use personal, sensitive or confidential information when working from home with the authorisation of your line manager.
- When working from home, ensure that information is used and stored securely and protected from access by family members or other visitors to your home at all times.
- Check the fax number before sending information via fax, particularly when using pre-set or speed-dial numbers.
- Ensure that e-mail addresses are correct before sending information via any e-mail method, particularly when addresses are auto-completed by your e-mail software.
- Know and apply the key Caldicott Principles to any information you are intending to send.
- Facilitate mobile / remote / agile working via secure method (NHS.net e-mail, encrypted memory stick, encrypted laptop etc). NEVER do this by e-mailing personal, sensitive or confidential information to a private / personal e-mail account or by storage on a non-Trust PC or laptop.

2.12 Caldicott Principles

The Caldicott Principles are 7 key principles which govern the use of patient data and offer best practice advice.

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don’t use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

All 7 principles have relevance to Safe Haven working, with the first 4 being particularly on point:

Justify the purpose – we must all be certain that what we are doing is necessary. We should not simply continue transfers of patient data ‘by wrote’.

Only use patient data when absolutely necessary – if the purpose can be achieved using fully anonymised data, do not use identifiers at all.

Use the minimum that is required – Establish the least amount of patient-identifiable data that supports the purpose and use this level of data, no more.

Access on a ‘need to know’ basis – Access to patient data should not exceed those whose roles require it. As an extension of this, patient information should not be sent to those that do not require it.

3 DUTIES AND RESPONSIBILITIES

The duties within the organisation are as follows:

Staff group	Duties
Chief Executive	The Trust Chief Executive will be responsible for signing off appropriate declarations on behalf of the Trust and will be ultimately accountable for Information Governance issues.
Senior Information Risk Officer (SIRO)	The Trust Senior Information Risk Officer (SIRO) is the Chief Financial Officer. The SIRO will act as the board-level owner of information risks and as such will be the point of contact for board level input in this area. Any difficulties in enacting this guidance and the resultant risks must be reported to the SIRO. The SIRO will be adequately trained via appropriate modules of the HSCIC IG Training Tool as a minimum, and will be supported by the Chief Information Officer and Information and Knowledge Services team in this role.
Caldicott Guardian	To be the Trust's ultimate authority on patient confidentiality issues. Will advise on patient data confidentiality matters and provide this expertise to the IG Group by attendance at IG Group meetings or delegation to a deputy officer. The Caldicott Guardian will be a board-level member of the executive team and will be appropriately trained to ensure that knowledge and expertise remains current. The Caldicott Guardian will be supported by the Information and Knowledge Manager in the role of Deputy Caldicott Guardian.
Information & Knowledge Manager	Will be the Trust's first line of Information Governance expertise and as such an active participant in the IG Group. Will author this guidance and act as first point of contact for advice on its content and the secure movement of confidential information.
IG Support Officer	Will assist the Information & Knowledge Manager as required and provide staff with support in relation to this guidance and the secure movement of confidential information.
Finance & Business Committee	Will support the IG team & IG Group in developing, enacting and ratifying IG-oriented procedures and provide a mandate for work in this area. Where necessary they will evaluate Trust progress in the area of information security and provide budgetary support of this guidance.
IG Group	Will support the IG team in developing and enacting this guidance and will provide a forum to debate future developments in this area. They will interpret and advise on appropriate action in the light of any new guidance coming from NHS England, HSCIC or the wider NHS. The group will be the appropriate reporting and investigatory body relating to IG incidents and will have oversight of the Trust IG Toolkit progress and reporting.

IG Team	Will continue to monitor the evolving Information Governance agenda and make recommendations to revise this guidance subject to need. The IG team will present any new directives in this area to the IG Group for consideration and action. The team will be responsible for providing any reporting to NHS England, HSCIC and any other relevant body. The team will lead operationally on IG Toolkit performance.
All staff	Will be personally responsible for making sure they adhere to the guidance at all times. Every member of staff and all personnel working with / for the Trust but not employed by the Trust have a personal responsibility to observe best practice in the storage, handling, communication and processing of all person-identifiable, sensitive and confidential information and remain vigilant to possible and actual breaches in confidentiality and report them through the Trust's incident reporting procedures. The Trust expects all staff to contribute to its determination to provide safe care and, in doing so, to uphold the statutory Duty of Candour and to meet the responsibilities articulated in their professional standards and in NHS and Trust Values. All staff should ensure that they are familiar with the requirements of the legal Duty of Candour, as set out in the Trust's Duty of Candour procedure CM-0060, available on staffnet.

4 TRAINING

Section 2 of this guidance gives staff procedural advice on the secure communication of personal, sensitive and confidential information. It is designed to supplement formal Information Governance training and act as a procedural reference guide. No additional training needs should arise, however the IG Team are available for guidance on the subject matter when required.

5 GLOSSARY OF DEFINITIONS

The following definitions are of relevance to this document:

Definition	**Meaning**
Agile Working	A working arrangement where staff no longer operate from a fixed base or office. Staff can operate via remote connection to Trust systems over secure links from mobile / remote locations.
Anonymised Data	Data with all identifiers removed such that data subjects within cannot be identified. This differs to pseudonymised data, which can be identified using a

	key. Truly anonymised data cannot be re-identified, even at source.
Confidential Information	Although Personal Information and Sensitive Personal Information are defined by the Data Protection Act (1998), other classes of information should be regarded as confidential and worthy of Safe Haven handling. These include confidential information relating to the Trust's business interests and activities, personal bank account details of staff and service users and any information which is given 'in confidence' or has the quality of confidentiality.
Government Secure Intranet (GSi)	An interconnecting secure communications infrastructure, providing secure and encrypted communications channels across the NHS and wider public sector. NHS.net e-mail is part of GSi.
Personal Confidential Data (PCD)	A term introduced by "Caldicott 2" in 2013. Whilst "personal" and "sensitive" data are defined by the Data Protection Act (1998), the Act's coverage does not extend post-mortem. PCD acknowledges the general principle that the confidentiality of medical records continues post mortem, and so adds to the DPA definition with inclusion of deceased service user records in a wider definition of what we must regard as confidential.
Personal Information	Information which may in itself, or alongside other information available from additional sources, be used to identify an individual. As defined by the Data Protection Act (1998).
Portable Digital Media	Memory sticks, recordable DVD / CD, flash memory cards and other electronic devices capable of holding data.
Pseudonymisation	A privacy-enhancing technology intended to produce an identifier which can only re-identify data subjects when the identifier is compared to the pseudonymisation key. Without the key, the data is anonymised.
Safe Haven	A working method or physical location which assures both sender and recipient that confidential information can be transferred with appropriate control. This will require a combination of a secure transit mechanism, delivery assurance, and access controls
Sensitive Personal Information	Information relating to race, ethnicity, religion or similar beliefs, sexuality, political affiliation, trade union membership, physical and mental health, and forensic history. As defined by the Data Protection Act (1998).

6 Appendices

Appendix A

Microsoft Office (2010) Document Encryption

Microsoft Office supports the encryption of documents to an acceptable standard for the encryption of personal, sensitive and confidential information.

- It should be used whenever personal, sensitive or confidential information is sent over otherwise unsecured e-mail systems (e.g. when sent outside of the NHS.net or wider GSi e-mail service).
- It may be used to enhance security of highly sensitive or confidential information when sent over secure e-mail systems.

We can encrypt MS-Office files to give the necessary protection using the following method.

1. Type up your MS-Word or MS-Excel file as normal
2. Left-click the “File” tab in the top left corner the screen
3. Left-click the “Protect Document” option in the resulting menu
4. Left-click “Encrypt with Password”
5. Type in your chosen password
6. You will be asked to re-type your chosen password for confirmation
7. Save your file
8. The recipient will need the password to unencrypt the file

Passwords should be communicated separately to the document itself.

- If e-mailing encrypted files, ask the recipient to e-mail you back for the password. Put this request in the body text of your covering e-mail.
- If posting encrypted files on portable media, ask the recipient to e-mail you for the password.

This step adds to security by assuring you that the file is in the hands of the right recipient.

DO NOT send the password with the encrypted file!

Although we have tested these methods with NHS.net mail accounts and found that MS-Office encrypted attachments can be both sent and received by our e-mail service, there is no guarantee that these methods will work with your intended recipients. Anti-virus measures may see the encrypted attachment as a potential threat and screen it out. Users are advised to test this method with a non-essential file to ensure it is workable.

Note: The Trust permits unencrypted e-mail communications with service users, carers and family members on completion of an informed consent process. See the Trust E-mail Use Policy.

Appendix B

NHS.net e-Mail [SECURE] Encryption Function

In 2015 NHS.net e-mail introduced an encryption mechanism to support the delivery of secure, encrypted e-mail communications beyond NHS.net and the wider Government Secure Intranet (GSi). This method may be used to deliver secure e-mail to otherwise unsecure addresses – such as service user personal e-mail addresses, solicitors and other non-GSi endpoints.

HSCIC have made available 2 guidance documents covering the use of the NHS.net e-Mail [SECURE] function, and these are available on the Trust intranet, links below:-

- NHSmail SECURE – Guidance for SENDERS
- NHSmail SECURE – Guidance for RECIPIENTS

The following instructions are taken from the HSCIC “Guidance for Senders”:-

How to send an encrypted message

Before sending patient or sensitive data via the encryption service, it is good practice to set up the ‘encrypted channel’ which helps safely verify the correct recipient.

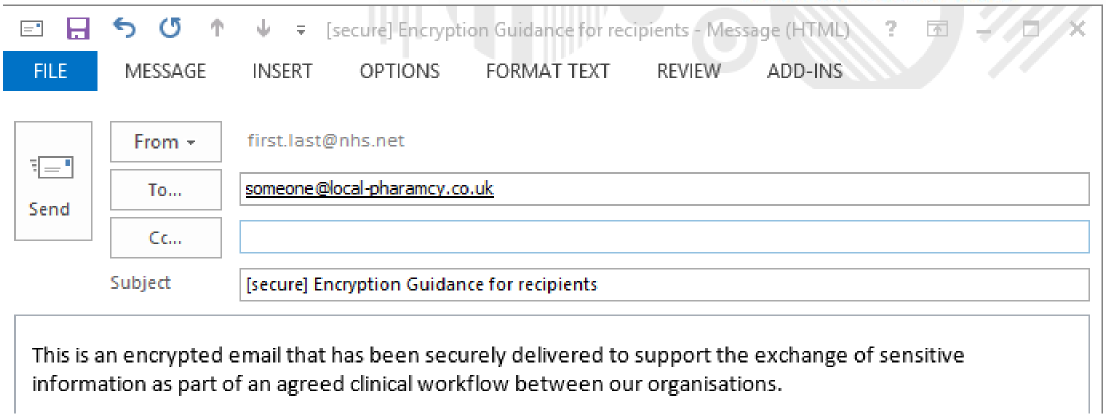
1. First, send the recipient the ‘Encryption Guidance for recipients’ document which you can find in the NHSmail Training and Guidance pages at: https://web.nhs.net/Portal/InformationGuidanceServices/DefaultPage.aspx in the section ‘Emailing sensitive or patient identifiable information’.

2. Next, follow the steps below to send an initial encrypted email but do not include patient or sensitive information. Once the recipient of the information has registered for the encryption service and confirmed to the sender this has been done, patient and sensitive data can be sent within an email or as an attachment subject to local information governance policies.

3. To send an encrypted email, log into your NHSmail account (either via an email client such as Outlook or via the web portal at www.nhs.net) and create a new email message in the normal way.

4. Ensure the recipient’s email address is correct.

5. In the **Subject** field of the email, enter the word [secure] before the subject of the message. The word secure **must** be surrounded by the square brackets for the message to be encrypted. If square brackets aren’t used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment.



From: first.last@nhs.net

To...: someone@local-pharamcy.co.uk

Subject: [secure] Encryption Guidance for recipients

This is an encrypted email that has been securely delivered to support the exchange of sensitive information as part of an agreed clinical workflow between our organisations.

6. Compose the message.

7. Add any required attachments (once the initial registration process has taken place).

8. Click on **Send** to send the message. An unencrypted copy will be saved in your **Sent Items** folder.

The service will then encrypt the message and deliver it to the intended recipient. The sent item will be stored unencrypted in your **Sent Items** folder, and any replies received will be decrypted and displayed as normal in NHSmail.

N.B. [secure] is not case sensitive and [SECURE] or [Secure] for example could also be used.

Users are advised to engage with both the senders and recipients guidance documents and to test this method with a non-essential e-mail to ensure it is workable.

PART B

7 PURPOSE OF DOCUMENT

7.1 Policy Statement

This document is intended as operational guidance. It relates to the Trust Information Governance Policy and forms part of the Trust approach to Information Governance and Information Security. It is part of the overall Information Governance Framework.

7.2 Purpose of Document

The guidance aims to provide operational instruction to those who send, receive and handle personal, sensitive and otherwise confidential information. Trust staff have numerous communication methods at their disposal. Given the Trust's core business often requires the movement of personal, sensitive and otherwise confidential information, it is imperative that the confidentiality of such information is maintained via the use of secure communications methods and staff whose own behaviours enhance our confidentiality culture and information security, via adopting a scalable approach to information security.

8 IDENTIFICATION OF STAKEHOLDERS

The table below should be used as a summary

Stakeholder	**Level of involvement**
All staff & associated personnel, who send, receive or handle personal, sensitive and otherwise confidential information	100%

9 REFERENCES, EVIDENCE BASE

- HSCIC IG Toolkit (Mental Health Trusts)
- NHS.net e-mail endorsements
- Data Protection Act (1998)
- The Caldicott Principles
- Royal Mail Letter / Parcel Services

10 ASSOCIATED DOCUMENTATION

- IG-0001 – Information Governance Policy
- IG-0003 – Confidentiality Code of Conduct
- IT-0001 – Encryption Policy
- IT-0003 – Email Use Policy
- IT-0005 – Portable Computing Device Policy

11 EQUALITY IMPACT ASSESSMENT

The general equality duty that is set out in the Equality Act 2010 requires public authorities, in the exercise of their functions, to have due regard to the need to:

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act.
- Advance equality of opportunity between people who share a protected characteristic and those who do not.
- Foster good relations between people who share a protected characteristic and those who do not.

Please complete the template by following the instructions in each box. If you require any guidance on how to complete the template please contact the Diversity and Inclusion Team on 0113 2954413.

Title:
Safe Haven Guidance

What are the intended outcomes of this work? *Include outline of objectives and function aims* Aim: To advise staff on secure communications methods and personal behaviours in respect of confidential information. Objective: To ensure that confidential information is moved securely and handled confidentially, according to Trust policy and procedure. Intended Outcomes: That breaches relating to confidential information are reduced in both frequency and severity, and that such breaches do not occur as a result of insecure communications or inappropriate working practices.
Who will be affected? *e.g. staff, patients, service users etc* Staff.

Evidence
What evidence have you considered? *List the main sources of data, research and other sources of evidence (including full references) reviewed to determine impact on each equality group (protected characteristic). This can include national research, surveys, reports, research interviews, focus groups, pilot activity evaluations etc. If there are gaps in evidence, state what you will do to close them in the Action Plan on the last page of this template.* Based on the knowledge of the author, the guidance is equally applicable to all, and discriminatory to none.

Disability *Consider and detail (including the source of any evidence) on attitudinal, physical and social barriers.* N/A
Sex *Consider and detail (including the source of any evidence) on men and women (potential to link to carers below).* N/A
Race *Consider and detail (including the source of any evidence) on difference ethnic groups, nationalities, Roma gypsies, Irish travellers, language barriers.* N/A
Age *Consider and detail (including the source of any evidence) across age ranges on old and younger people. This can include safeguarding, consent and child welfare.* N/A
Gender reassignment (including transgender) *Consider and detail (including the source of any evidence) on transgender and transsexual people. This can include issues such as privacy of data and harassment.* N/A
Sexual orientation *Consider and detail (including the source of any evidence) on heterosexual people as well as lesbian, gay and bi-sexual people.* N/A
Religion or belief *Consider and detail (including the source of any evidence) on people with different religions, beliefs or no belief.* N/A
Pregnancy and maternity *Consider and detail (including the source of any evidence) on working arrangements, part-time working, infant caring responsibilities.* N/A
Carers *Consider and detail (including the source of any evidence) on part-time working, shift-patterns, general caring responsibilities.* N/A
Other identified groups *Consider and detail and include the source of any evidence on different socio-economic groups, area inequality, income, resident status (migrants) and other groups experiencing disadvantage and barriers to access.* N/A

Engagement and involvement
How have you engaged stakeholders in gathering evidence or testing the evidence

available?
Stakeholder engagement plan

N/A

How have you engaged stakeholders in testing the policy or programme proposals?

N/A

For each engagement activity, please state who was involved, how and when they were engaged, and the key outputs:

N/A

Summary of Analysis *Considering the evidence and engagement activity you listed above, please summarise the impact of your work. Consider whether the evidence shows potential for differential impact, if so state whether adverse or positive and for which groups. How you will mitigate any negative impacts. How you will include certain protected groups in services or expand their participation in public life.*

Zero impact.

Now consider and detail below how the proposals impact on elimination of discrimination, harassment and victimisation, advance the equality of opportunity and promote good relations between groups.

Eliminate discrimination, harassment and victimisation *Where there is evidence, address each protected characteristic (age, disability, gender, gender reassignment, pregnancy and maternity, race, religion or belief, sexual orientation).*

N/A

Advance equality of opportunity *Where there is evidence, address each protected characteristic (age, disability, gender, gender reassignment, pregnancy and maternity, race, religion or belief, sexual orientation).*

N/A

Promote good relations between groups *Where there is evidence, address each protected characteristic (age, disability, gender, gender reassignment, pregnancy and maternity, race, religion or belief, sexual orientation).*

N/A

What is the overall impact? *Consider whether there are different levels of access experienced, needs or experiences, whether there are barriers to engagement, are there regional variations and what is the combined impact?*

Zero impact.

Addressing the impact on equalities *Please give an outline of what broad action you or any other bodies are taking to address any inequalities identified through the evidence.*

N/A

Action planning for improvement *Please give an outline of the key actions based on any gaps, challenges and opportunities you have identified. Actions to improve the policy/programmes need to be summarised (An action plan template is appended for specific action planning). Include here any general action to address specific equality issues and data gaps that need to be addressed through consultation or further research.*

N/A

For the record
Name of person who carried out this assessment:

Carl Starbuck – Information & Knowledge Manager

Date assessment completed: 22/12/2015

Name of responsible Director/Director General:

Dawn Hanwell – Chief Financial Officer (as SIRO).

Date assessment was signed: 22/12/2015

12 PLAN FOR DISSEMINATION AND IMPLEMENTATION

DETAILS OF DOCUMENT TO BE DISSEMINATED

Title of Document	Safe Haven Guidance		
Date Ratified	20/01/2016		
Dissemination lead name	Carl Starbuck	**Contact details**	carl.starbuck@nhs.net ext. 59771

DETAILS OF DISSEMINATION

Date put on Staffnet	20/01/2016			
Who is the document to be disseminated to	All staff			
Disseminated to (either directly or via meetings, etc)	**Format (electronic/ paper)**	**Date disseminated**	**No of copies sent**	**Contact details/comments**
Via intranet and trustwide e-mail	Electronic	TBC	1	carl.starbuck@nhs.net ext. 59771

13 Standards/key performance indicators

- By monitoring of performance against the HSCIC IG Toolkit. Progress reviewed monthly within the reporting year from publication (end June) to final submission (end March).
- By assessment of IG-related Incident Reports. Reviewed monthly by the IG Group

14 MONITORING COMPLIANCE WITH, AND THE EFFECTIVENESS OF THE PROCEDURE

Topic	Monitoring/ Audit	Lead Manager	Data Source	Sample	Data Collection Method	Frequency Of Activity	Review Body
HSCIC IG Toolkit	Audit	Carl Starbuck - Information & Knowledge Manager	HSCIC IG Toolkit returns	All requirements	Annual return	Annual	IG Group
IG incident reports	Monitoring	Carl Starbuck - Information & Knowledge Manager	DATIX / incident spreadsheet	All incident reports	Reporting to IG Group	Monthly	IG Group