Leeds and York Partnership
NHS Foundation Trust

SAFE HAVEN GUIDANCE

The key messages the reader should note about this document are:

1. Gives instruction to staff on how to move confidential information securely
2. Provides practical advice on using different methods of communication
3. Provides specific instructions on securing e-mail communications when sending outside of NHSmail
4. Informs the need for a scalable approach to secure communications
5. Gives advice on the behaviours and security awareness required when operating remotely or 'Agile Working'

This policy/procedure may refer to staff as qualified/registered/professional or other such term to describe their role. These terms have traditionally referred to individuals in a clinical role at band 5 or above. Please note that the use of these terms **may or may not** include nursing associates or associate practitioners (band 4). For clarification on whether a nursing associate or associate practitioner is an appropriate person to take on the identified roles or tasks in this policy/procedure please refer to the job description and job plan for the individual, or local risk assessment.

DOCUMENT SUMMARY SHEET
ALL sections of this form must be completed.

Document title	Safe Haven Guidance
Document Reference Number	IG-0009
Key searchable words	Safe Haven Guidance, e-mail, information security, fax, post, courier, encryption
Executive Team member responsible (title)	Chief Financial Officer (as SIRO)
Document author (name and title)	Carl Starbuck, Head of Information Governance
Approved by (Committee/Group)	Information Governance Group
Date approved	27/01/2022
Ratified by	Policy and Procedures Group
Date ratified	10 February 2022
Review date	10 February 2025
Frequency of review	*At least every three years*

Amendment detail

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
2.1	Review and update	Document at review date. Content aligned to GDPR, DPA (2018) and DSP Toolkit. Leeds City Council e-mail changes. NHS Fax end-of-life policy. Transferred to new procedural document template.
3.0	Ratified	Ratified by Policy & Procedure Group, 27 February 2019
3.1	Minor updates, including: Job Title Government & NHS E-mail standard references Secure public sector e-mail domain list Axe the Fax trajectory GDPR to UK GDPR Caldicott Principles O365 document encryption how-to NHS [Secure] instructions IG Group membership Minor proofing and language updates.	Reached 3 year review date
4.0	Ratified	Ratified by Policy & Procedure Group

CONTENTS

1. Executive Summary

The 'Safe Haven' concept is about the location and transport methods for personal, special category and otherwise confidential data being appropriately secure. Given the proliferation of transport mechanisms, the Trust approach to Safe Haven Working must encompass a wide array of communications methods. With the advent of an evermore agile workforce 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, special category or otherwise confidential information. In short, it's about each of us being a 'safe pair of hands' for the confidential information we use.

1.1 Flowchart of Procedure (if relevant)

Not appropriate for this guidance.

1.2 A Scalable Approach to Confidential Communications

The Trust accepts that there is a wealth of routine communication, by paper and electronic means which happens as business-as-usual. 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 the data we use and its storage and transfer. Further guidance should always be sought if you are unsure.

1.3 E-Mail

Confidential data should only be exchanged electronically when encrypted.The Trust uses NHSmail, which is the national secure e-mail service for health and social care. NHSmail email sent to secure domains is automatically encrypted and complies with the pan-government secure email standard. NHSmail is accredited to the secure email standard and is suitable for sharing patient identifiable and sensitive information.

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

NHSmail can communicate securely with other public sector domains. 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 Local / Central Government:

- *.gov.uk

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

- *.police.uk
- *.cjsm.net

Additionally, the NHS has an assurance standard against which organisations not using NHSmail can be accredited. NHS Digital is maintaining a list of e-mail domains which are encrypted & meet the Secure E-mail Specification (DCB1596), the list is available at the following link:-

https://digital.nhs.uk/services/nhsmail/the-secure-email-standard#list-of-accredited-organisations

E-mail sent to / from NHSmail addresses; the domains listed above, and domains listed as secure by NHS Digital will be encrypted in transit, giving us secure communications with various healthcare & public sector partner organisations.

When sending personal, special category or otherwise confidential information outside NHSmail to addresses other than the above, an alternative method of securing the information must be used. Appendices A & B detail alternative approaches to encryption that can be used to secure information when sent to unsecure e-mail addresses.

If you are in any doubt about whether a particular e-mail service is secure, contact the Head of Information Governance for advice.

1.4 Fax

Prior to the COVID-19 pandemic, the NHS started a project to bring the use of fax to an end. As of January 2019, no new fax machines could be bought, with the NHS aiming to phase out use of fax by 31st March 2020. 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 some partner organisations still use this legacy technology, and (at the time of writing) the impact of the ongoing COVID-19 pandemic has de-prioritised this objective, so fax use may persist.

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

Sending:-

- Personal, special category or 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 number, whereas incorrect manual

dialling will increasingly result in reaching a landline telephone rather than a fax.
- 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.

1.5 Internal Mail

Internal mail containing personal, special category 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 correspondence and confirming safe delivery with the recipient by phone or e-mail. Personal, special category 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, public or non-staff access.

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

External mail containing personal, special category 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 correspondence and confirming safe delivery with the recipient by phone or e-mail. Personal, special category 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, public or non-staff access.

It should be noted that point 1.2 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 1.7 below.

1.7 Traceable Mail Services and Courier Deliveries

Personal, special category 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, special category 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, only at posting and delivery.

1.8 Personal Delivery (By Hand)

Staff may elect to deliver personal, special category or otherwise 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 / collection.

1.9 Portable Digital Media / Document Encryption

Since the HMRC Child Benefit data loss in October 2007, the security of personal, special category or otherwise confidential information moved on portable digital media requires heightened scrutiny. Any personal, special category 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 procures hardware encrypted USB memory sticks. These sticks operate AES 256 bit encryption and are authorised for the transport of personal, special category 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.

1.10 The 'New Safe Haven' – Secondary Use Protection

The Trust 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 information security principles of the Data Protection Act (2018), the UK General Data Protection Regulation 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 e-mail is considered appropriate protection.

1.11 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, special category or otherwise confidential information.

Common sense practical steps will help us all to meet this legal 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, special category or confidential information from any vehicle on arrival at your work base, home, or final location.
- Only take & use personal, special category 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 Caldicott Principles to any information you are intending to send.
- Facilitate mobile / remote / agile working via secure methods (NHSmail, encrypted LYPFT laptop, Trust-issued encrypted memory stick etc). NEVER do this by e-mailing personal, special category or confidential information to a private / personal e-mail account or by storage on a non-Trust PC, laptop, or memory stick.
- Ensure that appropriate Trust policies and procedures are followed regardless of work location.

1.12 Caldicott Principles

The Caldicott Principles govern the use of personal data in health and social care and offer best practice advice. In terms of information security, Principles 1-4 align well with the information security principles of the Data Protection Act (2018) and the UK General Data Protection Regulation, by advocating the minimisation of identifiers; or their outright removal when their use is not justified, with Principles 5 & 6 underlining the obligations of staff to be aware of their personal responsibilities and to understand & obey the law as it applies to their work.

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.

8: Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

All 8 principles have relevance to Safe Haven working, with the first 6 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.

Be aware of your responsibilities – Trust policy, procedure, and your annual IG training inform you of your personal responsibility to protect confidential data.

Comply with the law – Failure to do so may result in regulatory or civil action.

1.13 Staff Duties and Responsibilities

All staff are 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 has a personal responsibility to observe best practice in the storage, handling, communication and processing of all person-identifiable, special category 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 the safe provision of 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.

1.14 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, including home.
Anonymised Data	Data with all identifiers removed such that data subjects cannot be identified. This differs to pseudonymised data, which can be identified using a key. Truly anonymised data cannot be re-identified.

Confidential Information	Personal and Sepcial Category Information are defined by Data Protection law, but 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, bank account and any information which is given 'in confidence'.
Personal Confidential Data (PCD)	Whilst Personal and Special Category data are defined by Data Protection law, coverage generally does not extend post-mortem. PCD acknowledges 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 (2018) and UK-GDPR.
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, access controls, and personal behaiviours.
Secure E-Mail Domain	E-mail services which are appropriately accredited as being secure when sending to or from NHSmail.
Special Category Information	Information relating to: Race and ethnic origin; religious or philosophical beliefs; political opinions; trade union memberships; biometric data used to identify an individual; genetic data; health data; sexual preferences, sex life, and / or sexual orientation, as defined by the Data Protection Act (2018) and UK-GDPR. Although defined separately in legislation, forensic data, e.g. offences, court appearances, police involvement etc. should be regarded as similarly sensitive.

2 Appendices

Appendix A - Microsoft Office 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 NHSmail or the secure domains referenced above).
- 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 2010 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

The method in MS-Office 365 is as follows:-

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 ‘Info’ in the resulting menu
4. Left-click the ‘Protect Document’ option in the resulting menu
5. Left-click ‘Encrypt with Password’
6. Type in your chosen password
7. You will be asked to re-type your chosen password for confirmation
8. Save your file
9. 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 NHSmail 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 - NHSmail [SECURE] Encryption Function

NHSmail has introduced an encryption mechanism to support the delivery of secure, encrypted e-mail communications to addresses outside of the secure domains quoted above. 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-secure endpoints.

NHSmail have made available 2 guidance documents covering the use of the NHSmail [SECURE] function, and these are available on the NHSmail portal, links below:-

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

The following instructions are taken from the NHS Digital 'Guidance for SENDERS':-

How to send an encrypted message

Exchanging patient / sensitive information should be done in accordance with local information governance policies and the NHSmail Acceptable Use Policy.

Before sending patient or sensitive data via the encryption service you should:

- Ensure that the recipient is expecting it and is ready to handle the contents appropriately, either as part of an agreed clinical or sensitive business workflow
- Send the recipient the accessing encrypted emails guide for non-NHSmail users, so they can register for the service
- Send an encrypted email as a test following the instructions below, but do not include patient or sensitive information the first time. This is to 'set-up' the secure channel of communication and ensure the correct recipient has successfully received the email. If it is an incorrect recipient, data has not been compromised.

Once you have established the secure channel of communication, patient and sensitive data can be sent within an email or as an attachment, subject to local governance policies.

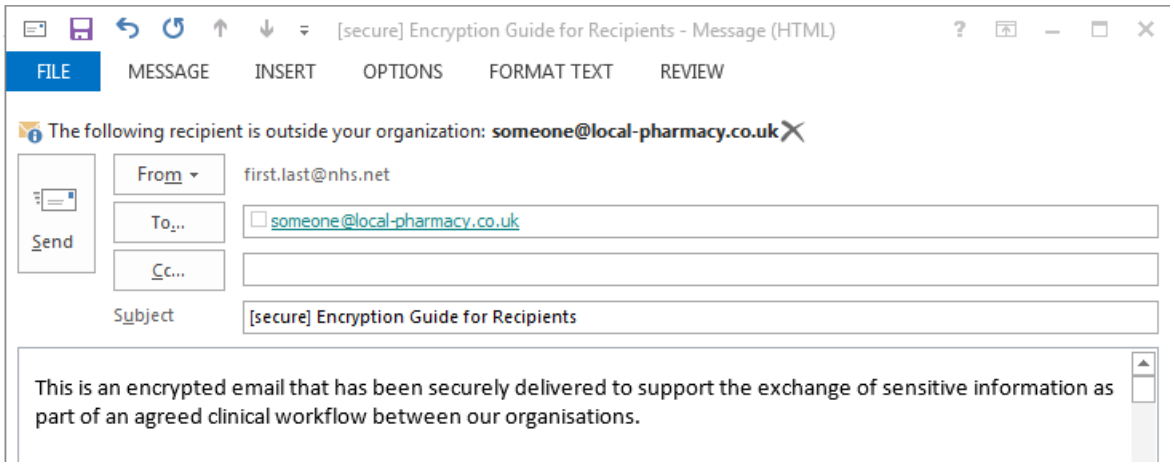
Some attachment types are not permitted to be sent via NHSmail, including .exe files. If a non-permitted attachment is detected it will automatically be removed. For the full list of nonpermitted attachments see the attachments guide.

Note: It is your responsibility and legal duty under the Data Protection Act 2018, on behalf of your employing organisation, to safeguard any data received in line with the

data protection and information governance requirements agreed between your organisation and the receiving organisation. If required, and in line with your local information management policies and processes, you should retain unencrypted copies of any encrypted email received in your local information repositories.

To send an encrypted email:

1. Log in to your NHSmail account (either via an email client such as Outlook or via the web portal at www.nhs.net).
2. Create a new email message.
3. Ensure the recipient's email address is correct.
4. In the **Subject** field of the email, enter the text **[secure]** either before or after the subject of the message. The word secure **must** be surrounded by the square brackets for the message to be encrypted.
   Note: If square brackets are not used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment.
5. Type the message.



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

Note: [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 to both parties.

PART B

3 IDENTIFICATION OF STAKEHOLDERS

The table below should be used as a summary. List those involved in development, consultation, approval and ratification processes.

Stakeholder	Level of involvement
Information & Knowledge Manager	Author / Subject Matter Expert
Information Governance Group (comprising) • Caldicott Guardian (or Deputy) • SIRO (or Deputy) • Head of Information Governance / Data Protection Officer / Freedom of Information Officer • Information Governance Support Officer • Chief Information Officer • Senior Information Manager • Human Resources Representative • ICT Network Support Manager • Head of IT Service Delivery • ICT Service Desk Manager	Consultation
Staffside Representatives	Consultation
Information Governance Group	Approval
Policy & Procedure Group	Ratification

4 REFERENCES, EVIDENCE BASE

- NHS Digital Data Security & Protection Toolkit
- Data Protection Act (2018)
- UK General Data Protection Regulation (GDPR)
- Sharing Sensitive Information Guide for NHSmail
- NHSmail [SECURE] guidance
- Royal Mail – Sending Mail – Your mail in safe hands

5 ASSOCIATED DOCUMENTATION (if relevant)

- IG-0001 – Information Governance Policy
- IG-0003 – Confidentiality Code of Conduct
- IG-0010 – Data Protection Policy
- IT-0001 – Encryption Policy
- IT-0003 – Email Use Policy
- IT-0005 – Portable Computing Device Policy
- IT-0008 – Information Security Policy
- IT-0010 - Mobile & Smartphone Communications Policy

6 STANDARDS/KEY PERFORMANCE INDICATORS (if relevant)

- Monitoring of performance against the NHS Digital Data Security & Protection Toolkit. Progress reviewed monthly within the reporting year from publication (May / June, annually) to final submission.
- Assessment of IG-related Incident Reports. Reviewed monthly by the IG Group.

7. EQUALITY IMPACT

The Trust has a duty under the Equality Act 2010 to have due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations between people from different groups. Consideration must be given to any potential impacts that the application of this policy/procedure might have on these requirements and on the nine protected groups identified by the Act (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, gender and sexual orientation).

Declaration: The potential impacts on the application of this policy/procedure have been fully considered for all nine protected groups. Through this process I have not identified any potential negative impacts for any of the nine protected groups.

Print name: Carl Starbuck

Job title: Head of Information Governance

Date: 11th January 2022

If any potential negative impacts are identified the Diversity Team must be contacted for advice and guidance: email; diversity.lypft@nhs.net.

CHECKLIST

To be completed and attached to any draft version of a procedural document when submitted to the appropriate group/committee to support its consideration and approval/ratification of the procedural document.

This checklist is part of the working papers.

	Title of document being newly created / reviewed:	Yes / No/
1.	**Title**	
	Is the title clear and unambiguous?	✓
	Is the procedural document in the correct format and style?	✓
2.	**Development Process**	
	Is there evidence of reasonable attempts to ensure relevant expertise has been used?	✓
3.	**Content**	
	Is the Purpose of the document clear?	✓
5.	**Approval**	
	Does the document identify which committee/group will approve it?	✓
6.	**Equality Impact Assessment**	
	Has the declaration been completed?	✓
7.	**Review Date**	
	Is the review date identified?	✓
	Is the frequency of review identified and acceptable?	✓
8.	**Overall Responsibility for the Document**	
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	✓

Name of the Chair of the Committee / Group approving			
If you are assured this document meets requirements and that it will provide an essential element in ensuring a safe and effective workforce, please sign and date below and forward to the chair of the committee/group where it will be ratified.			
Name	*Carl Starbuck*	Date	*11/01/2022*
Name of the chair of the Group/Committee ratifying			
If you are assured that the group or committee approving this procedural document have fulfilled its obligation please sign and date it and return to the procedural document author who will ensure the document is disseminated and uploaded onto Staffnet.			
Name	*Cath Hill*	Date	*10/02/2022*