# SAFE HAVEN PROCEDURE

| | |
|---|---|
| **Document Reference** | Proc452(IG) |
| **Version Number** | 4.0 |
| **Author/Lead**<br>**Job Title** | Karen Robinson<br>Information Governance Officer |
| **Lead Director name** | Peter Beckwith, Finance Director |
| **Consultation** | |
| **Date of Last Changes** | May 2022 |
| **Date of Next Review** | May 2025 |
| **Name of approving group/Committee/ Director**<br>**Date of approval** | Information Governance Group<br><br>May 2022 |

**VALIDITY – Policies should be accessed via the Trust intranet to ensure the current version is used.**

**CHANGE RECORD**

| Version | Date | Change details |
|---|---|---|
| *Proc V1.00* | *Nov 2016* | *Updated to a procedure as agreed at the IG Committee* |
| *Proc V1.01* | *September 2017* | *Updated 4.4 and Appendix A to require records to be sent Special Delivery as agreed at the IG Group September 2017.* |
| *Proc v2.0* | *September 2018* | *Reviewed and minor updates made. Additional information in 4.2.2 re Smartcards. Removed the requirement to keep manual data away from valuable equipment. Double checking handwritten/typed addresses. Advocating the use of email rather than fax. Updating emailing wording inline with the Electronic Comms Procedure. Use of the secure print facility on network copiers.* |
| *Proc v2.01* | *March 2019* | *Update 4.6 on secure email in line the updated Electronic Communications and Internet Acceptable Use Procedure* |
| *Proc v3.00* | *September 2019* | *Reviewed and updates made to 4.2.2, 4.3.2 and 10.1.7 in relation to electronic storage and removable media. Add to Section 4.5 that faxes can no longer be used from April 2020.* |
| *Proc v4.00* | *May 2022* | *Update scope to add that the procedure applies to staff working in Trust premises, shared office spaces and home working. Remove all references to fax machines. Add guidance to 4.2.1. on personal data in Outlook Calender. Update 4.2.2 to add guidance re shoulder surfing in public spaces/shared accomodations. Update 4.3.1 to advise that wherever possible, information required to support home working should be accessed electronically and to try not to print documents and work on them in public. Update 4.3 to include shoulder surfing, not allowing other member of the family to use a Trust device, not to leave equipment unattended, lock your work station when away from it. Update 4.4 to include a disclaimer for letters sent via the post. Update 4.6 in line with the latest Electronic Communications and Internet Acceptable Use Procedure. Update 4.7 in line with the NHS Transformation Directorate guidance on Protecting confidentiality and privacy on the telephone. Update 4.9 to advise staff home working to return confidential waste to a Trust base for secure disposal. Add a section in 4.10 on measures to take when home working. Approved by Information Governance Group (May 2022)* |

## Contents

## 1. INTRODUCTION

The Trust holds large amounts of confidential information that must be treated with respect and integrity. It is the responsibility of all members of staff to protect all personal and business sensitive data from inappropriate disclosure and access by adhering to the following Safe Haven Procedure.

This procedure supports the Information Security and Risk Policy and the Caldicott and Data Protection Policy.

## 2. SCOPE

This procedure applies to all employees of the Trust, including all staff who are seconded to the Trust, contract, voluntary, temporary and agency staff and other people working on Trust premises. This includes members of staff with an honorary contract or paid an honorarium.

The Trust promotes the safe haven culture for the protection and security of all personal data (including patient and staff data) and business sensitive data. Where this procedure refers to "records" this relates to any document containing personal or business sensitive information. The procedure also refers to all types of transfers including, for example, e-mail.

This procedure applies to staff working in Trust premises, shared office spaces and home working.

## 3. DUTIES & RESPONSIBILITIES

### 3.1 Chief Executive

The Chief Executive has overall responsibility for the effective implementation of this procedure.

### 3.2 Senior Information Risk Owner

The Senior Information Risk Owner will: -

- Chair the Information Governance Group.
- Represent confidentiality and security issues at Trust Board level.
- Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
- Take ownership of risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.
- Review and agree action in respect of identified information risks.
- Ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and/or discussion of information risk issues.
- Ensure the Board is adequately briefed on information risk issues.

### 3.3 Deputy Director of Finance

Deputise for the Senior Information Risk Owner as required.

### 3.3 Information Governance Team

Work with managers to review personal data flows within their work areas to ensure compliance with this procedure.

### 3.4 Managers

All Managers will: -

- Ensure that all work areas with their service comply with this procedure using the "Safe Haven checklist in Appendix B".

- Restrict access to personal information and business sensitive to named individuals (authorised users) who require the information.
- Review personal data flows within their work areas to ensure compliance with this procedure.
- Inform the Senior Information Risk Owner of ad-hoc bulk (more than 50 records) transfers of personal identifiable data.
- Ensure all personal/business sensitive data is securely transferred during any office moves. Final checks of drawers, cabinets and storage areas will be undertaken to ensure data is not lost or left behind.
- Disseminate the procedure to all members of staff.
- Display the Secure transfer by mail guidance in all mail areas.

### 3.5 Staff

All staff will: -

- Adhere to the following procedures.
- Wear ID badges/building passes.
- Query the status of strangers.
- Inform the line manager if anything suspicious or worrying is noted.

## 4. PROCEDURES

The Trust's Safe haven procedure for the security of personal and business sensitive information is:

### 4.1 Principles for Transferring Information

- Information must only be transferred for a justifiable purpose.
- The transfer must only take place when absolutely necessary.
- Only the minimum information necessary must be transferred.
- The information must be transferred on a need to know basis.

### 4.2 Physical Location and Security - Trust Premises

#### 4.2.1 Manual information

- Restrict access to any room where personal/business sensitive information is left unattended. If the room can be locked without compromising patient care then it must be locked. In areas where access cannot be restricted, for example reception desks, patient information must not be left on view.
- All post-rooms and post collection points must have physical security measures in place, for example, a key coded door.
- Only have the minimum information necessary on your desk for you to carry out your work. Any other related information must be put away securely, preferably locked away. This includes correspondence, removable media etc. Keys must be kept in a secret place known only to those who require access.
- Ensure that manual records are filed in readily accessible filing system which is understood by all members of the team, for example alphabetical. Further information on the referencing systems available can be found in the Records Management and Lifecycle Policy.
- Ensure that records are bound and stored with each piece of paper secure within the record folder.
- Store records closed when not in use in order that the contents are not seen accidentally.
- Ensure that each individual piece of paper is identified with the patient's surname, forename and NHS Number.
- Do not walk away from your work area leaving personal/business sensitive information exposed for unauthorised persons to see.
- Ensure that whiteboards and computer screens containing personal/business sensitive information are not visible to anyone approaching nurses' stations, reception desks or admission offices.

- Do not leave information left open in pigeonholes.
- If documents containing personal/business sensitive information come into your possession and you are not the intended recipient, you must either forward these to the intended recipient or, if this is not known, the Information Governance Team.
- Office diaries should be destroyed 2 year after the end of the calendar year to which they refer.
- Health Professional diaries, for example diaries used to record appointments with patients, should be destroyed 8 years after the end of the calendar year to which they refer. Diaries of clinical activity and visits must be written up and transferred to the main patient record.
- Any diaries containing personal information (both patient and non-patient information) should be destroyed under confidential conditions.
- Personal/business sensitive information must only be stored in your Outlook calendar if access is restricted to those who need to know this information. Only the minimum personal data should be used e.g. for a nurses appointments just the name or initials of the patient and the postcode if required. Consider marking entries as private, if not, all your delegates will have to the personal data in the entry.
- Outlook Calendar should not be used as a replacement for a health professional's diary. If an entry is accidently deleted from Outlook, there is no way to recover this information. Appointment details must be held in the relevant clinical system or a paper diary that is retained for 8 years.
- By default, Calendar Properties is set to show only free/busy times to other users of NHSmail. As this includes users outside of the organisation, this setting should not be changed to allow access to title, locations or all details of calendar entries.
- Report any loss of personal/business sensitive information to your manager and record the incident on Datix. Serious IG breaches regarding loss of data must also be reported to the Senior Information Risk Owner.

### 4.2.2 Electronic information

- Ensure that computer screens are not left on view so that members of the general public or staff who do not have a justified need to view the information can see the personal/business sensitive information.
- Use a screen protector to prevent shoulder surfing if you are in public spaces or shared accommodation when home working.
- Access to any PC must be password protected, this must not be shared or written down.
- Never share your smartcard and keep it secure at all times. A lost smartcard must be reported to the IT Service Desk as soon as possible.
- Lock your computer system when you leave your work area (do not wait for the screen saver to operate).
- Store electronic personal/business sensitive information in a secure folder on the Trust network or clinical system. Such information must only be saved on the local drive (C: Drive) of laptop computers temporarily for mobile access.
- Personal/business sensitive data must only be stored on Trust encrypted devices.
- Report any loss of personal/business sensitive information to your manager and record the incident on Datix.
- Use the secure print facility when printing personal/business sensitive information to network copier.

### 4.2.3 Dictation and Transcription Devices

- Tapes/SD cards holding any recording must be kept in a locked drawer/cabinet.
- Recordings must be kept for the minimum amount of time possible. Once the recording is transcribed or stored on the network, the recording must be completely deleted.
- Unencrypted media holding recordings must not be sent through the internal or external post.
- When in transit, the recordings must be carried in person in a secure locked case.
- Recordings must only be held on Trust equipment.
- All devices and tapes must be destroyed securely when no longer required.
- All new devices purchased must be encrypted.

### 4.3 Physical Location and Security When Working Away From Trust and Social Services Premises Included in the Mental Health Partnership Arrangement

#### 4.3.1 Manual personal/business sensitive information

Taking personal/business sensitive information away from Trust premises is a risk and should only be taken when absolutely necessary. Wherever possible, information required to support home working should be accessed electronically. Try not print documents and work on them in public spaces, they will be vulnerable to theft or misplacement. Personal data includes patient and staff information. See section 10.1 for full definitions.

If you need to take personal/business sensitive information away from the Trust, the following requirements need to be followed.

- Ensure you have authority to take the information. This will normally be granted by your line manager. Authorisation will only be granted when there is an operational requirement for the information to be taken away. For example, only health and social care records required for patients being seen in the community can be removed. Ideally, records should not be removed for general administration purposes, e.g. writing reports.
- If you are taking manual health records, please ensure there is a record that you have these records, where you are taking them and when they will be returned.
- Information must be removed for the minimum amount of time possible.
- Only take the minimum information required for the authorised purpose.
- The information must be stored and carried in a secure case (zipped and locked). Information must not be carried 'loosely' as this increases the risk of dropping them and losing something.
- The secure case must be stored in the locked boot of the car or carried on your person while being transported from your work place to your home. Such information must not be left overnight in a locked boot.
- Secure cases must never be visible in the boot of the car.
- Health records must only be taken home if the health or social care professional is not returning to their base after the working day or the records are required for the next working day. This must be with the prior agreement of the team manager.
- Health records must not be taken home for the purpose of delivering them to another base.
- Remember you are bound by the same rules of confidentiality whilst away from your place of work as you are when you are at your desk.
- When information is in the home, you have personal responsibility to ensure that it is kept secure and confidential. This means that other members of your family and/or your friends/colleagues must not be able to see this information or have access to it. The information must remain in the secure case.

#### 4.3.2 Electronic information

Laptop and mobile devices are vulnerable to theft. Trust devices must never be left unattended and must be stored in a locked boot whilst in transit. Such equipment must never be left overnight in an unattended car.

Loss or theft of a device must be report immediately to the IT Service Desk (01482 477877 – available 24 hrs) and the incident logged on Datix.

All portable devices e.g. laptops, tablets and smartphones must be encrypted and kept secure. Such devices must be procured through IT Services/Procurement to ensure they meet the Trust's encryption requirements

Removable media must be encrypted, must not be the only source of the information (i.e. the information must also be stored in a secure folder on the Trust network) and only used for secure transportation (i.e. not for routine work). Such media must be kept secure and not be identified as the property of the NHS. The password to the media must not be written down.

Removable media must only be purchased and installed by the IT Service Desk. Non-Trust owned removable media devices must not be used to store or transfer any confidential information. Each user of such media is responsible for the appropriate use and security of data stored on the media.

If removable media is used then the media must be encrypted and kept in locked storage. Unencrypted media must not be used to transport personal data.

If you take home non-identifiable information/non business sensitive on removable media, you must ensure that if you are putting this information onto your own PC that you take the information off again when you have finished your work.

Computerised person-identifiable information or business sensitive information must only be stored on and printed from Trust equipment e.g. a Trust encrypted laptop, a Trust encrypted memory stick.

Personal or business sensitive information stored on a Trust encrypted memory stick must be not transferred onto a non-Trust device, PC or laptop. Non-personal or non-business sensitive information, for example a PowerPoint presentation or report can be transferred onto a non-Trust device, PC or laptop.

Use a screen protector to prevent shoulder surfing if you are in public spaces or shared accommodation when home working.

Never allow anyone else such as family members to access your devices for personal use such as internet browsing.

Never leave equipment unattended, anywhere. Lock your workstation when away from it at home and in the office.

Do not open attachments in e-mails containing personal data/business sensitive information on equipment that doesn't belong to the Trust, even via the secure NHSmail web app.

For further information, please see Electronic Communications and Internet Acceptable Use Procedure.

### 4.4 Transfer of Information via Mail

- All information sent via internal/external mail must be in a **new** envelope, sealed and marked CONFIDENTIAL. All mail must be addressed to a named person and department. Old envelopes must not be used.
- The flow chart in Appendix A must be used to ensure the correct method of mailing is used e.g. internal, external, hand delivery, recorded or special delivery.
- Prior to sending any information to a patient's home address, confirm the address against the address recorded on a Trust system such as Lorenzo or SystmOne.
- For any handwritten or typed addresses, double check that is has been transcribed correctly before posting.
- All outgoing mail containing personal/business sensitive information must have a return address of : - Chief Information Officer, Humber NHS Foundation Trust, Trust Headquarters, Willerby Hill, Willerby, HU10 6ED in case of undelivered mail.All outgoing mail containing personal/business sensitive information must include the following disclaimer: *If you are not the intended recipient of this letter or any of its contents, please notify the sender asap who will arrange collection. Please be notified that any use, disclosure, copying or distribution of the information is prohibited.*
- Staff must nominate a colleague to open mail containing patient records when on annual leave. Such records must be kept secure in accordance with the procedures outlined in 4.2.1.

- Loose personal/business sensitive information must not be handed to another person for delivery simply because they are going to the destination department. It must only be delivered if the information is in a sealed envelope, marked confidential and to a named person.
- Where data is received in an insecure manner from an external/internal source, the recipient must notify that source and request that any future information must be sent securely. The incident must be reported on Datix.
- Do not pass documents containing information to other colleagues by leaving it on a secretary's desk or in an "IN" tray. Always ensure that information is in a sealed envelope addressed to the recipient and clearly marked **CONFIDENTIAL**.

**Additional requirements for Integrated health and social care records: -**

- Use Volume Tracking on Lorenzo to record the transfer of manual health and/or social care records.
- Please note that original Integrated Health and/or social care records must not be transferred outside the Trust. If a patient moves to another area the Medical Records Department will send a copy of the notes on request. The original record will be kept within the Medical Records Department. Records will be sent via special delivery.
- Records sent from the Medical Records Department will be traced to a named person at a unit or department. It is the named person's responsibility to ensure any subsequent movement of these records is recorded using the case note tracking system. This responsibility can be undertaken by one nominated person with a unit, for example an administrative member of staff working to a team of CPN's.

### 4.5 Transfer Of Information via Email

NHSmail provides of secure way of sending personal data/business sensitive information to other NHSmail users by email and Instant Messaging. It is one of a number of Government secure email systems. It connects securely to all of them allowing NHSmail users to share information confidently and securely with their users.

Emails can be sent securely to the following domains without any further action or protection, other than ensuring you have correct recipient:

- nhs.net
- gov.uk (no longer needs to be gsi.gov.uk, gcsx.gov.uk)
- cjsm.net
- pnn.police.uk
- mod.uk
- parliament.uk
- a domain accredited to DCB1596 Secure Email Standard (click here for list)

If sensitive information needs to be shared with a non-NHS Mail email address, staff should use Egress (enabled by including [secure] in the subject line), or using the Egress plug-in for Outlook.

Egress requires the recipient to register and create an account to be able to retrieve the files, and has the added advantage that i) the email and attachments are securely held within the Egress application, so are never actually 'sent' to the recipient, ii) it has a tracking feature which shows whether a recipient has accessed the email, and iii) has a 'revoke' feature which can be used to remove the previously sent email (effectively a 'recall' feature).

All personal data/business sensitive information sent outside of these domains should be sent using Egress by including [secure] in the subject heading or by using the Egress Outlook plug-in.. This includes emails sent to nhs.uk and nhs.scot email addresses.

Before using Egress:

- ensure that the recipient is expecting it and ready to handle the contents appropriately.
- Send the recipient the Accessing Encrypted Email Guide for non-NHSmail users so that they can register for the service.
- Send an email to the recipient with [secure] detailed in the subject heading of the email or by using the Egress plug-in for Outlook. At this stage, the email should not contain any personal/business sensitive data. The recipient will then be prompted to register with the encryption service.

Once the recipient has confirmed registration via an encrypted reply, personal data/business sensitive data can then be emailed. The email must still have [secure] in the email heading. Further information can be found at Encryption Guide for NHSmail.

This method should also be used when communicating by email with a patient/advocate. This must be with the explicit consent of the patient, see Section 3.10 Electronic Communications and Internet Acceptable Use Procedure.

Any breach of confidentiality resulting from using e-mail for personal identifiable data will be investigated and you are responsible for showing why any of the following guidelines may have not been applied. Messages containing personal data sent to the wrong recipient will be classed as a breach of confidentiality even if it is another NHS employee. Breaches should be reported on Datix immediately. It is possible to revoke access to an encrypted email sent using [secure] by following the Encryption Guide for NHSmail and changing the message status from “Active” and “Revoked”.

**Security measures**

- Make sure you have the correct recipient. If you are unsure, send a test email or asked the recipient to email you before sending any personal data.
- Mark the message appropriately in the subject line .e.g. “confidential” or “business sensitive” and select “confidential” in the Sensitivity section in the Message Options.
- Limit the number of recipients of the message to as few as possible.
- Limit the amount of data to only that which is needed for the purpose it is being sent e.g. use a unique identifier or initials instead of the person’s name.
- Manually select recipients from the address book and confirm their identity by checking the properties.
- Change the address book view to the Humber NHS Foundation Trust address list. This will avoid the chance of sending an e-mail to another employee in another NHS organisation with the same name.
- Send to e-mail addresses that are person specific unless the e-mail can be dealt with by any member of the team reading the e-mail. Be aware that e-mail can be forwarded by the initial recipient to third parties against your wishes or by accident.
- Include a note to say that the receiver of patient identifiable data is responsible for the security and confidentiality of that data and must not pass it on to anyone else, via any method, who does not have a justified ‘need to know’.
- Where there is a more formal method for the communication of information, such as ‘web-based’ referral system then that must be used.
- If you allow ‘delegate’ access to other people to your inbox, consider whether they need to see any personal data you receive.
- Anonymised information can be sent to non-secure email addresses, see Glossary of Terms for definition of anonymised.
- When in receipt of personal data remove it from your e-mail system as soon as possible and file it appropriately, either electronically or on paper.

- Review any attachments and make sure all are relevant to the recipients. Attachments containing confidential information not intended for disclosure should be sent separately from general attachments intended for dissemination.
- The file name for confidential attachments should include the word confidential at the beginning.

For further information, please see Electronic Communications and Internet Acceptable Use Procedure.

### 4.6 Transfer of Information by Telephone

When making or receiving telephone calls, for example, to set up an appointment, you need to follow simple safety precautions to ensure the privacy of the person you are calling.

- Double check the number before dialling.
- Ensure unauthorised people cannot overhear you when making sensitive telephone calls, during meetings, and when you are having informal discussions with colleagues about personal/business sensitive information. In these situations, if you do not need to identify a patient by name, then don't. If you are working from home, hold the conversation in a private space and use a headset.
- Ensure that the person you are calling cannot overhear other confidential matters in the background.
- Information must only be given over the telephone if you are confident of the identity of the caller. If you are not, you must always take a number, verify it independently and call back.
- When speaking to a patient or carer on the telephone, confirm the caller's identity by asking for two or three details such as their date of birth, postcode and the first line of their address.
- Ensure that recorded conversations on Trust answer-phones cannot be overheard or otherwise inappropriately accessed.
- Messages about named patients must not be left on answer-phones, unless previously agreed with the patient. Simply leave your name and telephone number and no other information.
- When receiving requests for information over the telephone, always check whether they are entitled to the information they request. Information on patients must only be released on a need-to-know basis. If in doubt, check with your line manager.
- If you receive suspicious queries regarding other members of staff asking about whereabouts, base or personal information, then please treat with caution, take contact details of the caller and either verify that it is an authorised person or pass the details to the individual concerned.
- If the person you are calling on the telephone challenges you and asks for proof of your identity: advise them to hang up, call your organisation switchboard, and ask for your extension number. You can then perform the simple identity verification checks described above. However, if you are calling from a potentially confidential or sensitive service, or have cause to be suspicious of the person's identity, consider using an alternative form of communication.
- Report any suspected bogus enquires to your line manager and via Datix.
- Message books to note messages for absent staff members must be stored securely.

**Protecting privacy when calling a patient's landline number.**

- When your call is answered: give your full name and the name of the organisation you are calling from, without specifics about the service or purpose of the call. Ask to speak to the relevant person by their full name.
- When the relevant person answers or comes to the phone: use the simple verification process described above to check their identity. Once you are satisfied you are speaking to the right person, tell them the service you are calling from and the purpose of the call.
- When someone else answers the phone: give your full name and the name of the organisation you are calling from, but not the service or purpose of the call. Ask if there is a better time to speak with the person and end the call, even if the recipient applies pressure to

extend it. Try calling again, at the suggested time if possible. Set a limit on the number of attempts made to call at different days and times and record them, before you consider sending a letter.

**Protecting privacy when calling a patient's mobile number.**

- Don't assume that mobile devices are more secure than landline telephones.
- Verify the person's identity using the simple verification process described above, before offering any details about the service you are calling from or purpose of the call.
- Check if you have called at an appropriate time and consider adjusting your questioning style to maintain privacy.

### 4.7 Transfer of Information Verbally

- When patients are registering for a service at a reception desk and are required to give personal/business sensitive information verbally ensure that this cannot be overhead by others.
- During ward rounds (or visits to nursing homes) when patient's details are being discussed, staff must bear in mind that they might be overheard by other patients in the same room. Whilst it is appreciated that it is difficult to manage confidentiality in situations like these, staff are expected to be aware of the possible problems and do all they can to respect the patient's rights.
- It is not appropriate to discuss personal/business sensitive information in corridors and stairways.

### 4.8 Disposal

When disposing of hand written or printed person-identifiable information, confidential, or business sensitive information, always use 'confidential waste' sacks/shredders. If possible, confidential waste should be shredded at source using a local cross cut shredder and then treated as waste paper.

Removable media containing confidential information can be physically destroyed using a shredder. Any other removal media requiring disposal should be hand delivered to the IT Service Desk for secure disposal.

Computer files with confidential information no longer required must be deleted from both the PC and the server if necessary. Computer hard disks are destroyed/ disposed of by the IT Services. Please contact the IT Service Desk for further information on 01482 477877.

When working from home, ensure any confidential waste is stored in a locked bag and returned to a Trust site for secure disposal.

### 4.9 Home Working

Additional measures to keep information safe and secure when working from home:

- Access information electronically, wherever possible.
- Use a screen protector to prevent shoulder surfing if you are in public spaces or shared accommodation.
- Never allow anyone else such as family members to access your devices for personal use such as internet browsing.
- Never leave equipment unattended anywhere and lock your workstation when away from it.
- Hold conversations in a private space and use a headset.
- Try not print documents and work on them in public spaces, they will be vulnerable to theft or misplacement.
- Ensure any confidential waste is stored in a locked bag and returned to a Trust site for secure disposal.

## 5. EQUALITY & DIVERSITY

An Equality and Diversity Impact Assessment has been carried out on this document using the Trust approved EIA The assessment indicates that there is little or no evidence/concern that the procedure will have a differential impact on any of the equality target groups.

## 6. IMPLEMENTATION

This procedure will be disseminated by the method described in the Policy and Procedural Documents Development and Management Policy.

This procedure does not require additional financial resource.

## 7. MONITORING & AUDIT

The Information Governance Team will implement an annual programme of site visits to audit compliance with this procedure. The findings will be reported to the Information Governance Group and appropriate corrective measures put in place. Any breach of the procedure will be monitored via the Reporting adverse incidents policy and procedure.

## 8. REFERENCES/EVIDENCE/GLOSSARY/DEFINITIONS

### 8.1 Definitions

#### 8.1.1 Safe Haven

Safe haven enables staff to be confident that information can be transferred to a secure environment. It means that the organisation has safeguards in place to ensure that unauthorised persons do not have access to information.

#### 8.1.2 Personal information - Patient Information

This includes one or more of the following: -

- Surname
- Forename
- Initials
- Date of birth
- Sex
- NHS Number
- Local identifier
- Address
- Postcode
- Telephone number
- National Insurance Number
- PID Number

It also includes pictures, photographs, videos, audio-tapes or other images of patients and anything else that may be used to identify a patient directly or indirectly e.g. rare diseases, drug treatments or statistical analyses which have very small numbers within a small population and may allow individuals to be identified.

#### 8.1.3 Personal information - Staff Information

Personal data about staff relating to their employment with the Trust.

#### 8.1.4 Personal information – other

Any information which identifies or relates to an individual.

#### 8.1.5 Business sensitive information

Information which, if compromised through alteration, corruption, loss, misuse or unauthorised disclosure, is likely to adversely affect the Trust or other third party (See Confidentiality Code of Conduct for employees in respect of confidentiality and information security for further information).

#### 8.1.6 Anonymised

Information that does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification.

#### 8.1.7 Removable media

Removable media includes: CDs, DVDs, optical discs, external hard-drives, USB Memory sticks (also known as pen drives or flash drives), Media card readers, embedded microchips (including Smart Cards and SIM cards), MP3 players, digital cameras, audio tapes, visual images (e.g. photograph) and media cards.

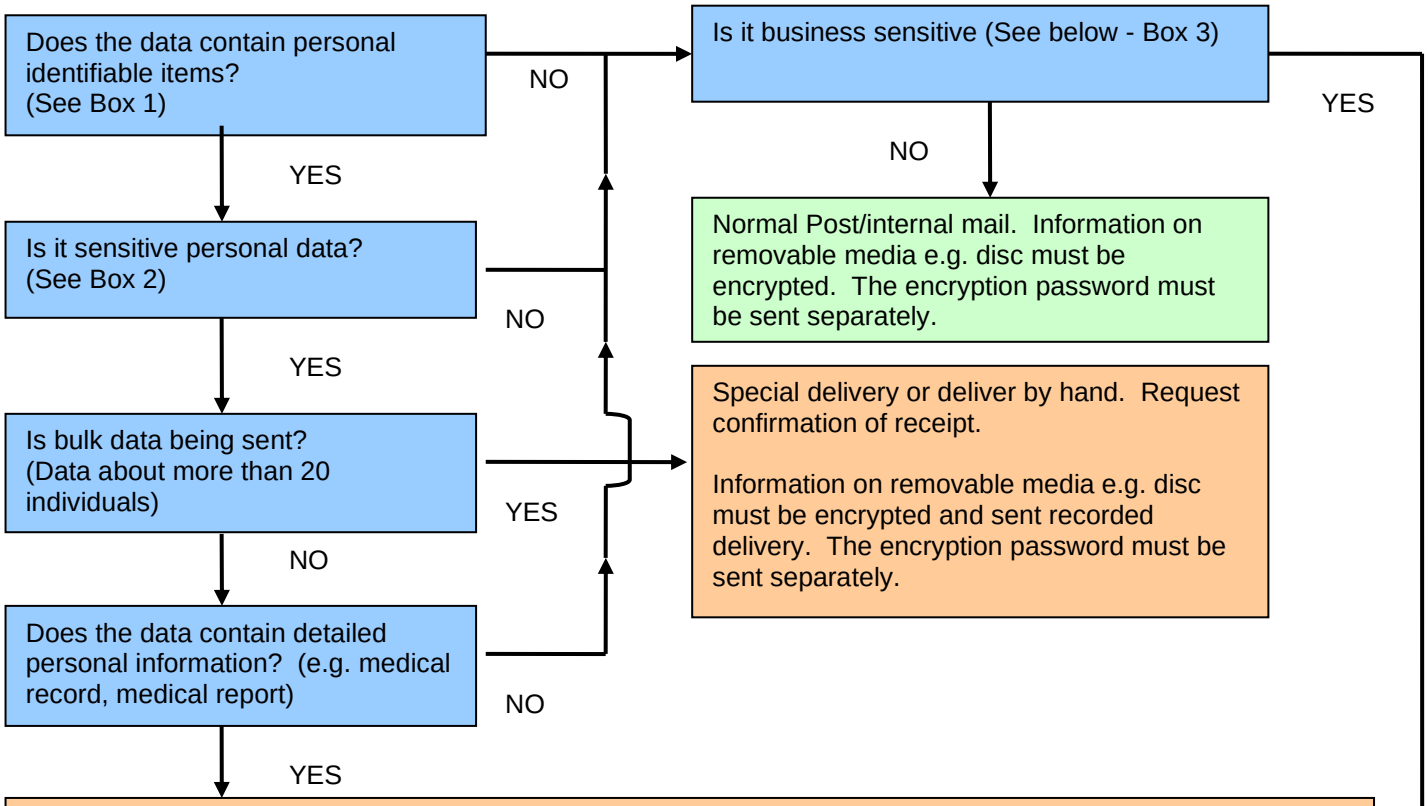
### 8.2 References

Data Security and Protection Toolkit.
NHS Transformation Directorate: Questions on protecting confidentiality and privacy on the telephone

## 9. RELEVANT HFT POLICIES/PROCEDURES/PROTOCOLS/GUIDELINES

Information Security and Risk Policy P096
Caldicott and Data Protection Policy P008
Confidentiality Code of Conduct P162
Electronic Communications and Internet Acceptable Use Procedure (Proc 451)

## Appendix A - Secure Transfer of Mail




Box 1 – Personal Data

Combination of one or more data items that would enable a person's identity to be established.

- Surname
- Forename
- Initials
- Date of birth
- Sex
- NHS Number
- Local Identifier
- Address
- Postcode
- Telephone number
- National Insurance No.
- PID Number

Box 2 – Sensitive Personal Data

Personal information containing any of the following types of information

- Physical or mental health
- Political opinions
- Religious beliefs
- Trade Union Membership
- Racial or ethnic origin
- Sexual life
- Commission of offences or alleged offences
- Other information that could adversely effect the individual

Bo

Information which, if compromised through alteration, corruption, loss, misuse or unauthorised disclosure could adversely effect the Trust or other third party. (See Confidentiality Code of Conduct)

## Appendix B - Checklist

### SAFE HAVEN CHECKLIST

Team Name ……

Base ……..

| | | |
|---|---|---|
| 1 | Is access to personal/business sensitive information restricted? | YES ☐ No ☐ |
| 2 | Is personal business sensitive information locked away? | YES ☐ No ☐ |
| 3 | Is the mail area physically secure? e.g. access restricted by a key coded door) | YES ☐ No ☐ |
| 4 | Are desks free of personal/business sensitive information (unless currently being worked on)? | YES ☐ No ☐ |
| 5 | Are screens on view to the public? | YES ☐ No ☐ |
| 6 | Are passwords individual and secure? | YES ☐ No ☐ |
| 7 | Are staff aware of smartcard security? | YES ☐ No ☐ |
| 8 | Do staff lock the screen when they leave the computer? | YES ☐ No ☐ |
| 9 | Is all personal/business sensitive data information on the Trust network? | YES ☐ No ☐ |
| 10 | Is there a system in place to track the removal/transfer of records (for health and social care records this must be the case note tracking system)? | YES ☐ No ☐ |
| 11 | Is electronic personal/business sensitive information held on removable media encrypted? | YES ☐ No ☐ |
| 12 | Do staff double check handwritten/typed mail addresses before posting. | YES ☐ No ☐ |
| 13 | Is the secure mail flow chart displayed in the mail area? | YES ☐ No ☐ |

| | | |
|---|---|---|
| 14 | Do staff understand the secure methods for sending personal/business sensitive data by e-mail? | YES ☐ No ☐ |

| | | |
|---|---|---|
| 15 | Do staff follow the “ring back” procedure before disclosing information over the telephone | YES ☐ No ☐ |
| 16 | Are answering machine messages left by patients secure (e.g. can they be overhead or inappropriately access)? | YES ☐ No ☐ |
| 17 | Are message books held securely? | YES ☐ No ☐ |
| 18 | Is paper-based personal/business sensitive information destroyed securely? | YES ☐ No ☐ |
| 19 | Are secure bags used to transport personal and business sensitive information? | YES ☐ No ☐ |
| 20 | Is the mail disclaimer including on patient letters? | YES ☐ No ☐ |

**Comments**

……

.....

……

.....

**Further actions**

……

.....

……

.....

**Completed by**

Name: ……Signature …….