Sherwood Forest Hospitals
NHS Foundation Trust

TITLE: Safe Haven Procedure

Document Category:	**INFORMATION GOVERNANCE**
Document Type:	**PROCEDURE**

Keywords:	Emails, destruction, security, USB

Version:	Issue Date:	Review Date:
5	March 2025	March 2027

Supersedes:	Version 4		
Approved by (committee/group):	Information Governance Committee	**Date Approved:**	18/03/2025

Scope/ Target Audience: (delete as applicable and/ or describe)	**Trust-wide**

Evidence Base/ References:	See Section 7)

Lead Division:	Corporate Services
Lead Specialty/ Department: (Or Division if 'divisionally' owned)	Information Governance
Lead Author: (position/ role and name)	Head of Data Security and Privacy
Co-Author(s): (position/ role and name if applicable)	
Sponsor (position/ role):	Caldicott Guardian

Name the documents here or record not applicable (these are documents which are usually developed or reviewed/ amended at the same time – i.e. a family of documents)	
Associated Policy	Email and Internet Policy
Associated Guideline(s)	
Associated Pathway(s)	
Associated Standard Operating Procedure(s)	
Other associated documents e.g. documentation/ forms	Email Guidance

Consultation Undertaken:	• Information Governance Working Group • Information Governance Committee

Template control:	V3 April 2024

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact 01623 672531 or email sfh-tr.information.governance@nhs.net

Amendments from previous version(s)

Version	Issue Date	Section(s) involved (author to record section number/ page)	Amendment (author to summarise)
4		Whole document	• No changes in practice

CONTENTS

	Description	Page
1	INTRODUCTION/ BACKGROUND	3
2	AIMS/ OBJECTIVES/ PURPOSE (including Related Trust Documents)	4
3	ROLES AND RESPONSIBILITIES	6
4	PROCEDURE DETAILS (including flowcharts)	7
5	EDUCATION AND TRAINING	14
6	MONITORING COMPLIANCE AND EFFECTIVENESS	15
7	EQUALITY IMPACT ASSESSMENT	16
8	APPENDICES Appendix A – Definitions	17

1 INTRODUCTION/ BACKGROUND

The term ‘Safe Haven’ is used within the NHS to denote either a secure physical location or the agreed set of administrative arrangements that are in place to ensure security classified, personal or other sensitive information is communicated safely and securely. Safe Haven processes have historically been associated with the use of fax but now extend to cover email, telephone calls, internal and external post. **Fax machines must not be used in the Trust.**

Safe Havens **should** be established, where:

- Information can be securely received and transferred.
- Paper-based information is stored securely in approved containers, as soon as practical.
- It is not on view or accessible to unauthorised persons.
- All waste potentially containing security classified, personal or other sensitive information is securely retained until it can be securely disposed of.
- Conversations discussing security classified, personal or other sensitive information can be held where they cannot be overheard by unauthorised persons.

The Trust has a duty of confidentiality when handling confidential information. Confidential information can be anything that relates to patients, staff or any other information (such as medical and staff records, contracts, tenders, etc.) held either in paper, disc, computer file or printout, video, photograph or even heard word of mouth. It includes information stored on portable devices such as laptops, mobile telephones and external hard drives/memory sticks). Personal information that is subject to a duty of confidence has a number of characteristics, i.e. the information:
• is not in the public domain or readily available from another source
• has a certain degree of sensitivity, (more than gossip) such as medical history
• has been provided with the expectation that it will only be used or disclosed for particular purposes. This expectation may arise because a specific undertaking has been given, because the confider places specific restrictions on the use of data which are agreed by the recipient, or because the relationship between the recipient and the data subject generally gives rise to an expectation of confidentiality, for instance as arises between a patient and a doctor.

All NHS organisations must have a Safe Haven Procedure in order to maintain the privacy and confidentiality of confidential information. Confidential information is transferred usually in one or more of the following formats:

- Computer systems
- Electronic mail (Email)
- Manual paper records
- Post and courier
- SMS Message
- Telephones/Answer Phones.

Confidential information, whether about a patient or a member of staff, is fundamental to the provision of confidential and effective services within the NHS.

We are all involved with the processing of confidential information, directly or indirectly during our employment with the NHS and **it's our duty to keep this information private and an individual's right for the confidentiality of their information to be respected**.

2 AIMS/ OBJECTIVES/ PURPOSE (including Related Trust Documents)

This procedure provides:

- The legislation and guidance which dictates the need for a safe haven
- A definition of the term safe haven
- When a safe haven is required
- The necessary procedures and requirements that are needed to implement a safe haven
- Rules for the different types of safe haven
- Who can have access and who you can disclose to.

Processing[1] confidential information is based on eight Caldicott principles:

1. **Justify the purpose for using confidential information** - Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.
2. **Use confidential information only when it is necessary** - Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.
3. **Use the minimum necessary confidential information** - Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.
4. **Access to confidential information should be on a strict need-to-know basis** - Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.
5. **Everyone with access to confidential information should be aware of their responsibilities** - Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.
6. **Comply with the law** - Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

[1] Almost anything we do with data counts as processing, including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

7. **The duty to share information for individual care is as important as the duty to protect patient confidentiality** - Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users 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.

Every day the Trust collects vast amounts of confidential information about our patients and staff. This information does not belong to the Trust; it belongs to the people that it has been collected from. The Trust is merely the custodian. As custodians we are responsible for the safe keeping and security of all confidential information that comes into our keeping.

This procedure supports compliance with the UK General Data Protection Regulation and Data Protection Act 2018 which imposes personal responsibilities on those who handle confidential information.

Related Trust Documents

- Email and Internet Policy
- Email Guidance
- Information Security Policy
- Data Protection, Confidentiality and Disclosure Policy.

A number of Acts and good practice guidance requires safe haven arrangements to be set in place, they include:

Data Protection Act 2018 (Principle f): Integrity and confidentiality (security). Ensure that you have appropriate security measures in place to protect the personal data you hold. This is the 'integrity and confidentiality ' principle of GDPR – also known as the security principle.

Code of Practice on Confidential Information[2]:
"Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are secure as they can be"

The Caldicott Guardian Manual[3] – the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be

[2] https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/code-of-practice-on-confidential-information

[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf

shared with external bodies both within, and outside, the NHS. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related IT Systems, disclosure to research interests and disclosure to the police.

Information Security Management: NHS Code of Practice[4] – all individuals who work within, or under contract to, an NHS organisation have a general responsibility for the security of information that they create or use in the performance of their duties

NHS Information Governance – Guidance on Legal and Professional Obligations[5] – this document lists the relevant legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed

3 ROLES AND RESPONSIBILITIES

All individuals who work within, or under contract to, an NHS organisation have a responsibility for the security of confidential information that they create or use in the performance of their duties.

The **Chief Executive** has overall responsibility for this policy within the Trust. Implementation of, and compliance with this policy is delegated to the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, and members of the Information Governance Committee. Trust Board has responsibility, in compliance with the Trust's Governance manual, to ensure and gain assurance that the Trust has in place robust arrangements for the management of records and that such arrangements are complied with.

The **Director of Corporate Affairs** is responsible to the Chief Executive for Information Governance and is the designated Senior Information Risk Owner, who takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the Board and provides written advice to the Chief Executive on the content of the Statement of Internal Control in regard to information risk. The Senior Information Risk Owner also reports annually to the Trust Board on Information Governance performance.

The **Chief Medical Officer** is the 'conscience' of the organisation, providing a focal point for patient confidentiality, information sharing and advising on the options for lawful and ethical processing of information as required.

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is

[4] https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/information-security-management-nhs-code-of-practice
[5] https://digital.nhs.uk/binaries/content/assets/legacy/pdf/o/s/nhs-information-governance-legal-professional-obligations.pdf

added and what is removed, how information is moved, and who has access and why. As a result, they can understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process. Record Management responsibilities will be written into all accountable individuals' job descriptions.

Information Asset Administrators (IAAs) ensure that Information Governance policies and procedures are followed, recognise actual or potential Information Governance security incidents and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, they seek the advice of our Data Protection Officer who also monitors the process. Information Asset Administrators will liaise with the Information Governance Team on the management of records in that directorate/speciality/department. The Information Governance Team will provide support and guidance to nominated departmental representatives.

All staff (including Medirest, Skanska, agency, and contractor colleagues) who use and have access to confidential information must understand their responsibilities for data protection and confidentiality. Whatever level of access is required by an individual, it is important that all handling of information only takes place on a strictly need to know basis.

The **Information Governance Committee** is responsible for ensuring that this procedure is effectively implemented, including any supporting guidance and training deemed necessary to support the implementation and for monitoring and providing assurance in this respect.

4 PROCEDURE DETAILS (including Flowcharts)

4.1 Email Communications

Before you open an email, consider whether you are the intended recipient.

If you suspect that you have received a phishing email, please contact the IG team or NHIS for further advice.

All emails must be sent securely.

NHS.net to NHS.net
NHS.net emails are secure (encrypted).

Any email sent from one NHS.net email account to another is secure (e.g. ginarobinson1@nhs.net to sfh-tr.sar@nhs.net.

NHS.net to other public sector agencies

Emails are secure when delivered to any of the following email addresses from NHS.net:

- **nhs.uk:** but only if they are listed here
- **cjsm.net:** used by public sector agencies
- **gcsx.gov.uk:** used by local councils for secure information exchange
- **gov.scot:** used by public sector organisations in Scotland
- **gov.uk:** used by UK public sector organizations, such as central government departments and parish councils
- **gse.gov.uk:** used by the United Kingdom government for secure email
- **gsi.gov.uk:** used by the United Kingdom government for secure email
- **gsx.gov.uk:** used by the United Kingdom government for secure email
- **llyw.cymru:** used by public sector organisations in Wales
- **mod.uk:** used by public sector agencies
- **parliament.uk:** used by public sector agencies
- **police.uk:** used by public sector agencies

NHS.net to non-secure emails

If you are in doubt as to whether the email is being sent to a secure email address **you must** use [SECURE] (the word secure must be surrounded by square brackets) in the email subject line when sending from NHSmail. This will secure (encrypt) the email and its contents. Responses from the email recipient will also be secure when replying back to you. Guidance is available here: Encryption Guide for NHSmail. There is also guidance for email recipients which is available here: Accessing Encrypted Emails Guide.

Email guidance

- All emails must be processed in line with the Email and Internet Policy and associated guidance.
- Users must ensure that confidential information is sent to the correct email address of an individual/shared mailbox. All email addresses registered in NHSmail have the employing organisation associated with the individual.
- You must ensure that any attachments, for example, Excel spreadsheets are double checked for any backing data, hidden cells or other sheets in a spreadsheet document that must be removed (if appropriate) prior to sending.
- Users must confirm the email address and spell any awkward words and where appropriate send a test email. Once the email has been sent, recipients should confirm receipt either via return email or telephone.

In all instances the following guidelines must be followed:

- Consider if email is the most appropriate method to send the information.
- Consider whether individuals/departments could be given access to a secure area on the shared (network) drive where the information can be securely stored for those with appropriate access to view.
- Where possible, limit the number of recipients based on the ‘need to know’ principle.
- Double check that you have the correct recipient(s) before pressing the “send” button.

- Messages containing confidential information sent to the wrong recipient will be classed as a breach of confidentiality even if it is to another NHS employee, as they do not need to see that information. An incident will need to be logged in all cases.
- Reduce the amount of confidential information to only that which is necessary for the purpose it is being sent. Do not send more, just in case the recipient needs it and always double check any attachments before sending.
- Add the word 'confidential' in the subject line as well as selecting the sensitivity (confidential) of the message in the Tags menu.
- Be aware that your emails may be forwarded by the recipient to third parties.
- **Use the minimum necessary confidential information** - Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.
- Consider using a unique identifier or the initials of the individual(s).
- Consider whether the information could be pseudonymised (NHS number/assignment number replaced with a number) or anonymised (all patient or staff identifiers have been removed).
- When in receipt of confidential information, take appropriate steps to action the contents. NHSmail is **not** a storage area.
  Where there is a more formal method for the communication of confidential information, such as 'web-based' referral system or a restricted Teams channel then that should 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 (all patient or staff identifiers have been removed) information can be sent via email outside the organisation.

4.3 Post

External and internal

Confidential information sent within or outside of the Trust must be subject to the following procedures:

- Before any mail is sealed and sent it should be ensured that the information is correct, and no additional papers or documentation for other individuals have been included within the envelope.
- All mail containing confidential information must be sent in a securely sealed envelope and marked as 'PRIVATE & CONFIDENTIAL'. This also applies to all staff correspondence.
- If you are sending confidential information in re-used envelopes, you must ensure that only the recipient's address is clearly visible to avoid confusion on delivery i.e. cross out or cover any previous address details.
- Consider if the post is the most appropriate method to send the information.

- Consider whether individuals/departments could be given access to a secure area on the shared (network) drive where the information can be securely stored for those with appropriate access to view.
- For batches / bulks[6] of confidential information use recorded delivery and / or courier. Always ask the recipient to confirm receipt.

Internal post only

- It is acceptable to add your details as a return address in case the envelope does not reach its intended recipient. This should be marked as "If undelivered please return to……" This may be beneficial for confidential staff information i.e. HR information, Payroll etc. When sending patient case notes through the internal post, it is acceptable to use a securely sealed envelope. This must be labelled with the recipient's full name, job title, department and location. **Staff HR files must be hand delivered to HR upon staff terminations.**
- When sending large volumes of case notes it is good practice to use sealed green boxes, which are available from Case Note Store. These should also be clearly labelled with the recipient's details.
- Before sending anything confirm the recipient's location. Staff should contact those to whom they are sending confidential information, to ensure that the correctly marked envelope will be sent to a specific individual and location. If possible and practical, please consider whether the confidential information should be delivered in person to ensure prompt and secure transfer.
- The post room staff will ensure all confidential information is delivered to the named individual and not left with anyone else.
- Confidential information must not be opened by anyone other than the addressee unless authorised to do so. Staff who normally receive confidential information must ensure that adequate arrangements are in place to take receipt of mail during periods of holidays and sickness.
- Ensure the seal is secure – for example, stick a piece of sellotape / sticky tape over the seal rather than tucking the seal into the envelope as documents can easily fall out and be lost during transportation.
- It is good practice to use double envelopes when sending confidential information.
- It is good practice to keep a record of what you have sent so you can track when you sent it just in case of loss or queries.
- With regards to recruitment and interview information, please ensure any personal files, personal data, interview packs which may include photographic ID evidence, bank details, home address verification are hand delivered to HR.

External post

- When sending confidential information mark the envelope 'Private & Confidential – To be opened by Addressee Only'.

[6] (a batch of data or bulk data is defined as data relating to 51 or more individuals, or a quantity of data sent / received in a single consignment , variable according to sensitivity)

- Open incoming mail away from public areas. Mail must be opened by the addressee only if marked as such.
- Routine appointment letters to individual patients does not need to be sent by verified email (using [secure] function see Email Guidance Version 1) or recorded or special delivery, except where the information is particularly sensitive (such as copies of medical records)
- Confirm the name, department and address of the recipient prior to sending and ask the recipient to acknowledge receipt of the information.
- Seal the information in a robust envelope using strong wrapping tape.
- If the information is of a particularly sensitive nature or the number of patients involved exceeds 10 persons (is “bulk” data), then the mail should be sent by recorded delivery (signed for delivery) or special delivery (signed for and tracked and trace throughout the delivery cycle). A risk assessment should be made to decide on which method (recorded or special delivery) should be used.
- Deliver confidential information immediately or as soon as possible to the recipient but do not leave on the desk or pass to anyone else if the recipient is not available. Lock in a drawer or cabinet until the recipient is available.

4.4 Telephone

Incoming calls may provoke sensitive/confidential conversations. Exercise caution to ensure sensitive conversations are not overheard, and that only appropriate information is discussed.

Confidential information received over the telephone must be processed appropriately, in accordance with existing standards and/or legislation.

If the use of a telephone is essential to convey sensitive information, then the following security protocols must be adhered to:

- Ensure that the enquirer has a legitimate right to have access to the information before information is given out and provide information only to the person who has requested it.
- Confirm the name, job title, department and organisation of the person requesting the information, ensuring that you are speaking to the correct person.
- Take a contact telephone number e.g. main switchboard number **(never a direct line or mobile telephone number if possible).**
- Ring back to confirm that person’s identity.
- Confirm the reason for the request.

4.5 Answer phone / Voice mail messages

We encourage the use of telephone communications with patients and service users to support the delivery of care. 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.

Further information is available in the Data Protection, Confidentiality and Disclosure Policy, section 6.8.

The dangers of leaving messages are:

- Who might hear the message?
- Are you sure that you have telephoned the correct number?
- Will the recipient fully understand the content of the message?
- Can you be certain the message has been received by the patient?
- You may inadvertently breach patient confidentiality because the patient's friends or relatives may not know the patient is receiving health care.

4.6 Face to face conversations

When patients are registering for a service at a reception desk and are required to give confidential information verbally, wherever possible ensure this cannot be overheard by others.

During ward rounds when patients' details are being discussed, staff should bear in mind that they might be overheard by other patient's 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 confidential information in corridors, stairways and lifts or any public areas.

4.7 Face to face requests for patient information

You may be asked the whereabouts of a patient e.g. if you are working on a reception area.

- Establish the fullest details of the patient as a means of establishing the authenticity of the enquirer
- Ask the relationship of the enquirer and patient
- Ask what department / ward they think the patient may be attending and ask them to take a seat for a moment
- Try to ascertain the whereabouts of the patient
- If you manage to locate the patient, telephone the department and ask permission from the patient to send the enquirer / relative to that area if it is appropriate or pass the message on that they are here waiting.

4.8 Physical location and security

Further information is provided in section 6 of the Information Security Policy.

4.9 What information can you give to relatives / personal representative (next of kin)?

- With your agreement we will share information about your current care with your family or carer. It is important that we know which family members or carers to involve in your care, and who we can share your information with. This person does not need to be related to you, but they should be able to tell us your wishes in case you are unable to do so yourself.
- Check the identity of the caller and the patient's full name whom they are enquiring about Think about the information you may be giving out, clinical details should not be given out without consent of the person concerned, always remember the patient may not want this information being passed on to other relatives / friends
- Explicit consent should be gained from patients regarding who they are happy for staff to discuss their health matters with. If this is not possible owing to the patient's condition, staff members will be required to make their own judgment and may be required to justify their decision, any decisions made must be recorded in the patient record.
- Confidential information should only be given if disclosure is to an authorised source, and it is known exactly why it is required. Callers should be questioned if necessary and if the member of staff is in any doubt as to their identity or the reasons for wanting the information they should offer to ring the caller back, using a number obtained from an independent source, such as the patient demographic system (PAS) and/or passes the call on to a manager. **There should be no hesitation about doing this; any bona fide caller would expect it.**
- Any concerns that a caller may not be who they say they are, or that they are asking for information they are not entitled to must be escalated to your line manager and, if necessary, the Information Governance team. Under these circumstances no information should be disclosed.

Please note: Within any area of work there will be a designated person responsible for routine flows of information. If you have not dealt with a request previously, or you are unsure, you must seek advice.

4.10 What information can you give to other Health and Social Care staff?

- Check identity of the member of staff – their name, department and the nature of the enquiry – do they need to know the information and have a justified reason for asking for the information – remember the Caldicott principles
- Request their telephone number and call them back
- If there is a genuine need for confidential patient information to be released be aware of others who may be listening
- If you are unsure of the callers identity and do not know how to proceed talk to your manager or contact the Information Governance Department.

4.11 What information can you give to patient's employers?

No information can be given to the patient's employers without the explicit[7] consent of the patient concerned. Refer any such enquiries to the Information Governance or Human Resources Department. Further guidance is available from the Information Commissioner's Office: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/

4.12 Data Transfers

- Only approved transfer methods shall be used.
- An approved method of encryption shall be used for the transfer of OFFICIAL – SENSITIVE data that is sent outside the secure network.
- Where possible data transfers should always be carried out over existing, protected and trusted NHS networks, however, there may be occasions where data will need to be transferred over other networks. On these occasions Trust staff **must** request guidance from a member of the Information Governance Team as the data files **must** be protected by encryption to protect the data should it fall into the hands of unauthorised persons.

5 EDUCATION AND TRAINING

Training
Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition all existing staff must undertake data security awareness level 1 training on an annual basis. Staff can undertake online. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018 to include General Data Protection Regulations (GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the Information Governance team.

Implementation
A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website.[8]

[7] If confidential patient information is used for purposes beyond individual care, for example giving details to an employer, then it will normally be necessary for staff to obtain explicit consent. This is a very clear and specific statement of consent. It can be given in writing, verbally or through another form of communication such as sign language

[8] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/

6 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum requirement to be monitored	Responsible individual/ group/ committee	Process for monitoring e.g. audit	Frequency of monitoring	Responsible individual/ group/ committee for review of results	Responsible individual/ group/ committee for development of action plan	Responsible individual/ group/ committee for monitoring of action plan
Review of inventory of corporate records	Head of Data Security & Privacy , Information Governance Committee	Review	Annually	Information Governance Team	Information Governance Team	Information Governance Committee
Adherence DPA, FOI and other Information Governance areas	Head of Data Security & Privacy , Information Governance Committee	Monitor	Annually	Information Governance Team	Information Governance Manager	Audit & Assurance Committee

The Trust will regularly monitor its safe haven practices for compliance with this framework.

Local areas and services will audit their own practices from time to time, at least annually to measure compliance with this policy or in light of future requirements.

7 EQUALITY IMPACT ASSESSMENT (please complete all sections of form)

- Guidance on how to complete an Equality Impact Assessment
- Sample completed form

Name of service/policy/procedure being reviewed: Safe Haven Procedure			
New or existing service/policy/procedure: Existing			
Date of Assessment: 21st January 2025			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?	b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?	c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality
The area of policy or its implementation being assessed:			
Race and Ethnicity:	None	Not applicable	None
Gender:	None	Not applicable	None
Age:	None	Not applicable	None
Religion / Belief:	None	Not applicable	None
Disability:	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request	None
Sexuality:	None	Not applicable	None
Pregnancy and Maternity:	None	Not applicable	None
Gender Reassignment:	None	Not applicable	None
Marriage and Civil Partnership:	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation):	None	Not applicable	None

What consultation with protected characteristic groups including patient groups have you carried out?

- None.

What data or information did you use in support of this EqIA? • None.
As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments? • No.

<u>Level of impact</u> Low Level of Impact

Name of Responsible Person undertaking this assessment: Gina Robinson
Signature: GR
Date: 21st January 2025

8 APPENDICES

APPENDIX A – DEFINITIONS

Personal Confidential data	This is a term used in the Caldicott Information Governance Review and describes personal information about identified or identifiable individuals, which should be kept private or secret and includes deceased as well as living people. The review interpreted 'personal' as including the Data Protection Act definition of personal data but included data relating to the deceased as well as living people, and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.
Personal Data	Personal data means information about a particular living individual 'data subject'. It does not need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data. It does not cover truly anonymous information – but if you could still identify someone from the details, or by combining it with other information, it will still count as personal data. It only includes paper records if we plan to put them on a computer (or other digital device) or file them in an organised way. In the Trust, all paper records are technically included – but will be exempt from most of the usual Data Protection rules for unfiled papers and notes. Examples of personal information include: • a name • identification number i.e. NHS number, NI number • location data • an online identifier i.e. IP addresses and cookie identifiers • one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Almost anything we do with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.
Special categories of personal data (previously known as sensitive data, Data Protection Act 1998)	• Biometrics • Criminal convictions • Ethnic origin • Genetics • Health information • Politics

	• Race • Religious beliefs • Sexual life • Sexual orientation • Trade union membership For this type of information even more stringent measures should be employed to ensure that the date remains secure
Safe Haven	The term ‘Safe Haven’ is used within the NHS to denote either a secure physical location or the agreed set of administrative arrangements that are in place to ensure security classified, personal or other sensitive information is communicated safely and securely
Staff	Means all employees of the Trust including those managed by third party organisation on behalf of the Trust
The Trust	Sherwood Forest Hospitals NHS Foundation Trust