Sherwood Forest Hospitals
NHS Foundation Trust

Safe Haven Procedure

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

Keywords:	Safe Haven, Fax, Emails, Destruction, Security, USB

Version:	**Issue Date:**	**Review Date:**
3	February 2023	February 2024

Supersedes:	Safe Haven Policy Version 9		
Approved by (committee/group):	Information Governance Committee	**Date Approved:**	30th January 2023

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

Evidence Base/ References:	NHS Digital
Lead Division:	Corporate Services
Lead Specialty:	Information Governance
Author:	Information Governance Manager
Sponsor:	Chief Executive

	Name the documents here or record not applicable
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 Version 1

Consultation Undertaken:	Information Governance Working Group Information Governance Committee

Template control:	v1.3 January 2018 (Supports the Trust's 'Policy for Policies')

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 mailto:sfh-tr.information.governance@nhs.net

Contents

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. Historically Safe Haven processes have been associated with the use of fax but now extend to cover email, telephone calls, internal and external post. **The use of fax is now not available to 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 or destroyed.
- Conversations discussing security classified, personal or other sensitive information can be held where they cannot be overhead by unauthorised persons.

The Trust has a duty of confidentiality when handling personal confidential data and all NHS organisations require a Safe Haven Procedure in order to maintain the privacy and confidentiality of personal confidential data. Personal confidential data may be transferred via the following formats:

- Computer systems
- Electronic mail (Email)
- Manual paper records
- Post and courier
- Removable media e.g., laptops, CDs,
- SMS Message
- Telephones/Answer Phones

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

We are all involved with the processing of personal confidential data 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 policy provides:

The legislation and guidance which dictates the need for a safe haven

- A definition of the term safe haven
- When a safe haven is required
- The necessary procedures and requirements that are needed to implement a Safe Haven
- Rules for different kinds of safe haven
- Who can have access and who you can disclose to

The principles for transferring information (based on Caldicott Principles 1-8)

1. Information should only be transferred for a justifiable purpose
2. The transfer should only take place when absolutely necessary
3. Only the minimum information necessary should be transferred
4. The information should be transferred on a need to know basis
5. Everyone with access to confidential information should be aware of their responsibilities
6. Comply with the law
7. The duty to share information for individual care is as important as the duty to protect patient confidentiality
8. Inform patients and service users about how their confidential information is used

Every day the Trust collects vast amounts of personal confidential data about patients and staff. The information is not the property of the NHS or 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 information that comes into our keeping.

The implementation of these procedures facilitates compliance with the legal requirements placed upon the organisation, especially concerning special categories of data (e.g. people's medical condition).

Related Trust Documents

- Email and Internet Policy
- Email Guidance Version 1
- Information Security Policy
- Data Protection & Confidentiality Policy

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

Data Protection Act 2018 (Principle 6): Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Code of Practice on Confidential Information[1]:
"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[2] – the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be 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[3] – 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[4] – 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 information that they create or use in the performance of their duties

The **Chief Executive** is accountable for the safe use including transfer of personal confidential data and corporate sensitive data in the organisation, but all staff, contractors and temporary staff have a duty of confidence to maintain confidentiality.

The **Senior Information Risk Owner** (SIRO) has responsibility for understanding how the strategic business goals of the organisation may be impacted by any information risks.

The **Caldicott Guardian** is responsible for promoting patient confidentiality and clinical governance within the Trust.

[1] https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf
[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf
[3] https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf
[4] https://digital.nhs.uk/binaries/content/assets/legacy/pdf/o/s/nhs-information-governance-legal-professional-obligations.pdf

Information Asset Owners (IAOs) are senior individuals who can be held accountable should an information security incident occur within their department. The IAOs role is to understand and address risks to the information they 'own' and provide assurance to the SIRO.

Information Asset Administrators are responsible for supporting the IAOs to fulfil their responsibilities. These staff will ensure that policies and procedures are followed, recognise actual or potential security incidents, consult with IAOs on incident management and ensure that information asset registers are accurate and up to date.

All **Staff** including individuals from partner agencies working within multi-disciplinary teams who process information are responsible for ensuring personal confidential data/corporate sensitive data remains secure and confidential at all times. 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 to the Board

4 Procedure Details

It's a legal requirement to document our processing activities. To take stock of what information the Trust holds and ensure we know what we have, where it is and what we do with. We must also ensure that we have a valid lawful basis and justify its purpose.

Data mapping exercises are undertaken annually within each area and forwarded to the Information Governance Team for review.

4.1 Email Communications

All email **shall** be sent over an encrypted network such as the Health & Social Care Network.

NHS.net to NHS.net

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

NHS.net to other public sector agencies excluding NHS

NHS.net email is hosted on the Health & Social Care Network and as such forms part of the wider public sector Government Secure Intranet (GSi). This means that email is encrypted when delivered to any of the following email domains: **@pnn.police.uk, @pnn.gov.uk, @secure.nottscc.gov.uk**

NHS.net to non-secure emails

If you are in doubt as to whether the email is being sent to a secure email address use [SECURE] [5](this must be square brackets) in the email subject line when sending from NHSmail. This will automatically encrypt the email. The response from the recipient will also be secure when replying to you.

Email guidance

- All emails must be processed in line with the Email and Internet Policy and associated guidance.
- Users must ensure that any confidential information is sent to the mailbox of a person authorised to see that information and that no unauthorised persons have access to that mailbox.
- Confidential or special categories of personal data should not be sent to shared or group email boxes unless completely sure of the user group members and their security arrangements.
- When sending confidential information, staff must not include personal confidential data in the heading or main body of an email. Please ensure that any attachments are double checked for any personal/ sensitive/ confidential information. This could include any backing data, hidden cells or other sheets in a spreadsheet document.
- Users must confirm the email address and spell any awkward words and where appropriate send a test message. Once the message has been sent, recipients should confirm receipt either via return email or telephone.

In all instances whether the email is encrypted or not, the following guidelines must be observed:

- Consider if email is the best way to send the data. For example, an alternative is if the recipient can access the same shared drive as the sender the document could be placed on the network drive for both to access.
- Limit the number of recipients of the message to as few as possible
- Double check that you have the correct recipient(s) before pressing the “send” button.
- Messages containing personal data sent to the wrong recipient will be classed as a breach of confidentiality even if it is another NHS employee as they do not need to see that information. This can be done by checking the “properties” of the recipient you have selected
- Limit the amount of data to only that which is needed for the purpose it is being sent. Do not send more, just in case the recipient needs it and double check any attachments for additional or hidden information before sending.
- Mark the message as ‘confidential’ in the subject as well as in the message properties
- Be aware that your email can be forwarded by the initial recipient to third parties against your wishes or by accident
- Use the minimum personal identifiable information, particularly in subject titles and

[5] http://www.mansfieldandashfieldccg.nhs.uk/media/1984/email-guidance-how-to-send-an-encrypted-email-to-gmail-nhsuk-hotmail.pdf

document names e.g. use a unique identifier or initials instead of the person's name
- Include a note to say that the receiver of patient identifiable data is responsible for the security and confidentiality of that data and should not pass it on to anyone else, via any method, who does not have a justified 'need to know'
- When in receipt of personal data remove it from your email system as soon as possible and file it appropriately, either electronically or on paper
- Do not keep personal data on email for longer than is necessary
- Where there is a more formal method for the communication of information, such as 'web-based' referral system 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 information can be sent via email outside the organisation

Please note: wherever possible any transfer of personal confidential data should contain the minimum amount of data required, or either anonymised or pseudonymised.

Further guidance is available from the Information Governance Internet site:

- **Email and Internet Policy**
- **Email Guidance**

4.3 Post

External and internal

Confidential mail 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 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.
- For batches / bulks of confidential and personal data (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) use recorded delivery and / or courier. Always ask the recipient to confirm receipt.
- If CD's or removable media such as pen drives must be sent via the post as a last resort which contain personal confidential data, ensure this is encrypted using the methods available to you. If the data cannot be encrypted, more stringent security measures should be taken to transport it such as by courier or hand delivery.

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 and department.
- When sending large volumes of notes it is best 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 address. Staff should contact those to whom they are sending confidential information, to ensure that the correctly marked envelope will be sent to a specific post-holder at a specific location. If sending highly confidential and sensitive information, telephone the recipient or ask them to confirm with you that the mail has been received. If possible and practical please consider whether the information should be delivered in person to ensure prompt and secure transfer.
- The Trust staff sorting post will ensure all confidential mail is delivered to the named individual.
- Confidential mail must not be opened by anyone other than the addressee unless authorised to do so. Post holders who normally receive confidential mail must ensure that adequate arrangements are in place to take receipt of mail during periods of holidays and sickness.
- Ensure the seal is tamper proof – 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 personal / sensitive internal mail.
- 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 personal confidential data mark the envelope ‘Private & Confidential – To be opened by Addressee Only’.
- Routine appointment letters or mail 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 with the Information Governance lead should be made to

decide on which method (recorded or special delivery) should be used, the Information Commissioners Office only recognises special delivery as a secure form.
- Deliver confidential incoming post 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.
- Open incoming mail away from public areas. Mail must be opened by the addressee only if marked as such.

4.4 Telephone

Incoming calls may provoke sensitive/confidential conversation. 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

If you are required to contact a patient by telephone, it is good practice to obtain consent from the patient in advance to establish whether they are happy for you to leave a message, if necessary. This consent and specific requirements are to be recorded in their health record.

If you are required to leave a message on patient's answer phone / voice mail without prior consent, for example, the cancellation of an appointment at short notice, you are not to mention the fact that you are ringing from the Trust or leave any clinical information. The only information you are to leave is your name, telephone number and a brief message asking them to call you back.

Staff are not to leave messages for patients if there is any doubt regarding the validity of the telephone number.

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.

Additional safeguards

- Take steps to protect a patient's confidentiality whilst speaking on the phone
- Ask questions over the telephone that require the patient to answer rather than giving details which they need to confirm.
- Do not repeat any information given to you out loud
- Put callers on hold if necessary so that they can't hear other confidential conversations that may be going on in the background
- Always ensure before information is given out that the enquirer has a legitimate right to have access to the information – remember you cannot take it back once it has been given out
- Do not have the phone switched to 'speaker' mode turning a confidential call into a 'tannoy' message
- Ensure that recorded conversations on answer phones cannot be overheard or otherwise inappropriately accessed.

4.6 Face to face conversations

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

During ward rounds when patient's 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 personal confidential data 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

- Records will be stored in locked drawers or cabinets, in a locked office area with a swipe card door entry security system, limited to staff working for the Trust. A nominated person will be responsible for the security of locked cabinets where personal confidential data are stored within individual business teams. They will be responsible for the safe-keeping of the information stored in the cabinets. They should not be left in areas where unauthorised access could occur i.e. public corridors.
- All business areas that have personal confidential data must have an appropriate Safe Haven and ensure that it meets appropriate standards (i.e. that it complies with Data Protection Legislation, in particular with reference to Principle 6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'); and Caldicott Principle 4 'Access to patient identifiable information should be on a strict need-to-know basis').
- Teams that have a Safe Haven storage facility within their own work areas should ensure an appropriate tracking system is in place for all information stored in the facility. The person removing the information is then responsible for maintaining its confidentiality and returning it as quickly as possible to its storage place.
- All data (with the exception of hard copy transfers) shall be stored encrypted (using a Trust approved method).
- An approved method of transfer shall be determined for the type of data being transferred.
- Removable media shall only be authorised when there is a valid business requirement.
- Only official Trust approved removable media shall be used.
- Where information is transferred via mail the outer envelope/package shall not be marked with its Security Classification.
- Transfers of data in hard copy form will need to be protected, by using such methods as approved couriers or Royal Mail Track and Trace. Where data is to be transferred by memory stick, CD/DVD or removable hard drive, the media should be encrypted to 256bit, which will provide adequate protection should it become lost or fall in to the hands of unauthorised persons.
- Unauthorised people will not be allowed access to areas where confidential information is kept unless supervised. ID badges will be checked before access is permitted.
- Door and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level.
- Computers should not be left on view or accessible to unauthorised staff
- Screen savers should be activated (Ctrl+Alt+Delete then Enter) when the computer is not in use or be switched off when not in use.
- Restrict access to any room where personal confidential data is left unattended. If the room

can be locked without compromising patient care then it should be locked. In areas where access cannot be restricted e.g. reception desks patient information should not be left on view.

- Only have the minimum information necessary on your desk for you to carry out your work. Any other related information should be put away securely. This includes correspondence, cd, memory sticks etc. Keys should be kept in a secret place only known to those who require access.
- Do not walk away from your work area leaving personal confidential data exposed for unauthorised persons to see and ensure computers are locked when not in use (Ctrl+Alt+Delete, then enter).
- Do not leave personalised data left open in pigeonholes
- If documents containing personal confidential data come into your possession and you are not the intended recipient, you should forward these to the intended recipient if known informing them that it was sent to you in error, if this is not known then return the information to the sender. An incident to be recorded on DATIX the Trusts incident reporting system.

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

- 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
- 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
- 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 phone book 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 clinical 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 consent of the patient concerned. Refer any such enquiries to the Human Resources Department. Further guidance is available from the Information Commissioner's Office:

- The Employment Practices Code
- The Employment Practices Code Supplementary Guidance

4.12 Vocera communications

- The Vocera system is an "open" communication system, and output voice can be heard by anyone in close proximity to the badges at both the transmission and reception ends. It is important for users of the system to bear this in mind and be aware of the potential audience when engaged in conversations of a sensitive or confidential nature. Use of Vocera for dictation or retrieval of confidential or patient information, should only take place in a suitably private environment.
- Users of the system should adhere to their professional code of conduct and patient confidentiality when sharing patient information over the Vocera system.

4.13 Internet Data Transfers

- Only approved transfer methods shall be used and in accordance with the Security Classification of data.
- An approved method of encryption shall be used for the transfer of OFFICIAL – SENSITIVE data that is sent outside the secure network (see guidance in the Email policy … sending to non-NHSmail email addresses).

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 the data files must be protected by encryption in order to protect the data should it fall in to the hands of unauthorised persons.

4.14 Data disposal

- Information held on ICT systems **shall** be securely erased in accordance with Records Management Code of Practice for Health and Social Care 2021
- Information held in paper form **shall** be securely destroyed in accordance with the NHS Records Management Policy.

4.15 Other Data Handling

- Where there are occasions when new pieces of work require one time only data transfers or data storage, Trust staff **should** request guidance from a member of the Trust Information Governance Team.

5 Education and Training

Training
Good Information Governance Education, Training and Development is essential for the development and improvement of staff knowledge and skills relating to Records management, as well as all other strands of Information Governance

Annual Information Governance training is included as part of the Trust's Mandatory Training policy. Staff are informed of the need to understand the value of information and their responsibility for it by undertaking either face-to-face training delivered by an Information Governance representative or by undertaking the mandatory Information Governance module on the NHS Digital approved online training module. This training covers the importance of data quality, information security, corporate and medical records management, confidentiality, their legal duty, information laws, rights of access, and the patient's rights in terms of a right to privacy and choice.

The Trust, supported by the SIRO, Information Governance Manager and Training Education and Development Manager are responsible for the development and delivery of all aspects of Information Governance Training, including records management and is supported in its implementation by the Trust's Information Governance Committee. Information Governance Training is also included as part of induction. Tailored training can be delivered on an ad-hoc basis dependent on staff roles.

IMPLEMENTATION
The policy, once approved, will be included within the governance policy section of the Trust's intranet website.

COMMUNICATION

As part of their induction all new staff will be made aware of the Trust's Policies and this policy and procedure will be available on the Trust's internet site. Any changes to this policy and procedure will be communicated to staff via the team brief and additional information and training provided for managers as required.

6 Monitoring

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	Information Governance Manager	Review	Annually	Information Governance Team	Information Governance Team	Information Governance Committee
Adherence DPA, FOI and other Information Governance areas	Information Governance Manager	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, Diversity and Inclusivity and Impact Assessments

Equality Impact Assessment (EqIA) Form (please complete all sections)

- 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: New			
Date of Assessment: July 2018			
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:	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? None

Level of impact From the information provided above and following EqIA guidance document please indicate the perceived level of impact: Low Level of Impact

Name of Responsible Person undertaking this assessment: Information Governance Manager
Signature:
Date: January 2023

8 Appendices

APPENDIX 1 – 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 • ~~an~~ 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