South Central Ambulance Service
NHS Foundation Trust

SAFE HAVEN POLICY

South Central Ambulance Service NHS Foundation Trust
Unit 7 & 8, Talisman Business Centre, Talisman Road, Bicester, Oxfordshire, OX26 6HR

DOCUMENT INFORMATION

Author:	Barbara Sansom, Information Governance Manager
Consultation & Approval:	Staff Consultation 21 days Audit Committee: 10th September 2018 Board Ratification: N/A
Equality Impact Assessment:	April 2018 - Stage 1 Assessment undertaken – no issues identified
Data Protection Impact Assessment:	April 2018 – Initial/High Level Assessment undertaken – no issues identified
Notification of Policy Release:	All Recipient email Intranet Website
Date of Issue:	June 2019
Next Review:	June 2022
Version:	**5.2** renewal to include changes to fax use **5.1** no content changes – period extended to 30th June 2018 to allow for review under new DPA / GDPR rules **5.0** – content changes to reflect General Data Protection Regulations (GDPR) & Data Protection Act (DPA) 2018

Contents

1. Introduction

All NHS organisations require safe haven procedures to maintain the privacy and confidentiality of the personal information held. The implementation of these procedures assists compliance with the legal requirements placed upon the organisation, especially concerning sensitive information

Where other Trust locations, other Trusts or other agencies want to send personal information to a Trust department, they should be confident that they are been sent to a location which ensures the security of the data, a safe haven.

2. Scope

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 requirements that are necessary to implement a safe haven for different kinds of communication
- Who can have access and who you can disclose to and applies to:
- Anyone processing information on behalf of SCAS, including all staff employed by the Trust, contracted third parties, agency staff, students, trainees, secondees, locum staff, staff on temporary placements, volunteers. It applies to Non-Executive Directors and any individuals not directly employed by the Trust such as community responders or volunteers
- All information (manual and electronic), information systems, networks, application and SCAS locations
- All business functions within SCAS
- All organisations providing a service on behalf of SCAS
- All services commissioned by SCAS
- Anyone having access to the SCAS IT network.

3. Responsibilities for Implementing the Safe Haven Policy

Information governance roles and responsibilities are detailed in the Trust's Information Governance Policy. Responsibilities specific to this policy are outlined below:

3.1 Caldicott Guardian

The appointed Caldicott Guardian for the Trust must approve all procedures that relate to the use of patient information

3.2 Data Protection Officer (DPO)

The role of the DPO is to inform and advise the Trust of obligations under the Data Protection Act 2018. The DPO will monitor compliance with the policies of the Trust in relation to the protection of personal data and will train staff and raise awareness as the need arises.

The DPO acts as the contact point for the Information Commissioner's Office on issues relating to processing

3.3 Information Governance Manager

The Information Governance Manager is responsible for coordinating improvements in data protection, the confidentiality code of conduct and with the Head of Information Security & Governance for information security matters.

3.4 All Trust staff

All staff that process personal-identifiable information and Managers who have responsibilities for those staff must adhere to this policy.

4. Definitions

4.1 Safe Haven

The term safe haven is a location (or in some cases a piece of equipment) situated on Trust premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely.

4.2 Personal Information/Data

Personal information is information which can identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private, for example name and private address, name and home telephone number.

4.3 Special Category Information/Data (previously described as sensitive personal information/data)

Special Category/sensitive personal information is where the personal information contains details of that persons:

- Health or physical condition
- Sexual life
- Ethnic origin
- Religious beliefs
- Political views
- Criminal convictions

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

5. Requirements for Safe Havens

Employees of the Trust authorised to disclose information/data to other organisations outside the NHS must seek an assurance that these organisations have a designated safe haven point for receiving personal/special category information. The Trust must be assured that these organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance documents (see 6. Key Legislation below)

Staff sharing personal/special category data/information with other agencies should be aware of protocol agreements made with, for example, Police Forces and Social Services.

5.1 Location/security arrangements

- A location should be a room that is locked or accessible via a coded key pad known only to authorised staff or
- The office or workspace should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to any members of staff who work in the same building or office, or any visitors
- Where the location is sited on the ground floor, any windows should have locks on them
- The room should conform to health and safety requirements in terms of fire and safety from flood, theft or environmental damage
- Manual paper records contained person-identifiable information should be stored in locked cabinets
- Computers should be not left on view or accessible to unauthorised staff and must have a secure screen saver function and be switched off or locked when not in use.

5.2 Fax machines

In January 2019 the Health & Social Care Secretary banned the NHS from purchasing fax machines and tasked it with phasing out fax use completely by April 2020. In the very few instances where there is no alternative but to transfer personal information via fax, the following rules must apply:

- The fax is sent to a safe location where only staff that have a legitimate right to view the information can access it.
- The sender is certain that the correct person will receive it and that the fax number is correct.
- The recipient is notified when the fax is being sent and acknowledges receipt once it has been sent
- Care is taken when dialling to ensure the correct number is used and wherever possible, pre-programme numbers into machines to prevent misdialling
- Confidential faxes must not be left lying around for unauthorised staff to see
- Only the minimum amount of personal information should be sent, where possible the data should be anonymised or a unique identifier used
- Faxes sent should include a front sheet, which contains a suitable confidentiality clause and a named contact/recipient
- Fax machines in the safe haven should have a code password and be turned off out of office hours.

5.3 Communications by post

- All sensitive records must be stored face down in public areas and not left unsupervised at any time
- Incoming mail should be opened away from public areas
- Outgoing mail (both internal and external) should be sealed securely and addressed to a named recipient and marked “private and confidential”

5.4 Computers

- Access to any PC must be password protected, this must not be disclosed or shared
- Computer screens must not be left on view so members of the general public or staff who do not have a justified need to view the information can see personal data.
- PCs or laptops not in use should be switched off or locked with a secure screen saver device in use.
- Information should be held on the Organization's network servers, not stored on local hard drives. Departments should be aware of the high risk of storing information locally and take appropriate security measures.
- All personal information sent by e-mail should be encrypted/password protected
- Clinical information must be clearly marked
- Check and double check email recipient addresses
- Browsers are safely set up so that for example, passwords are not saved and temporary internet files are deleted on exit
- The receiver is ready to handle the information in the right way
- Information sent by email will be safely stored and archived as well as being incorporated into patient records
- There is an audit trail to show who did what and when
- There are adequate fall back and fail-safe arrangements
- Information is not saved or copied into any PC or media that is "outside the NHS", particularly an individual's personal device(s)
- Great care should be taken in sending personal information especially where the information maybe of a clinical nature – it should be password protected and procedures undertaken to ensure that the correct person has received it.

Please also read the Trust's Email policy and Confidentiality Policy for more guidance on sending of personal information electronically.

6. Key Legislation

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

- GDPR and DPA 2018
  (Principle 7): "Appropriate technical and organisational measures shall be taken to make personal data secure"
- NHS Code of Practice: Confidentiality
  Annex A1 Protect patient Information *"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"*
- Common Law Duty of Confidentiality
- Caldicott Principles.

7. Linked Policies

- Lifecycle Policy (Records Management – the receiving, creating, handling, retention, sharing and destruction of records)
- Data Protection Policy
- Confidentiality Code of Conduct (rules for the use of, access to and disclosure of data/records)
- Information Sharing Agreement Protocols
- Information Governance Policy
- Confidentiality Policy
- IM&T Policies & Procedures (including email policy)
- Staff sharing personal/special category data/information with other agencies should be aware of protocol agreements made with, for example, Police Forces and Social Services.

8. Equality Statement

8.1 The Trust is committed to promoting positive measures that eliminate all forms of unlawful or unfair discrimination on the grounds of age, marital status, disability, race, nationality, gender, religion, sexual orientation, gender reassignment, ethnic or national origin, beliefs, domestic circumstances, social and employment status, political affiliation or trade union membership, HIV status or any other basis not justified by law or relevant to the requirements of the post.

8.2 By committing to a policy encouraging equality of opportunity and diversity, the Trust values differences between members of the community and within its existing workforce, and actively seeks to benefit from their differing skills, knowledge, and experiences in order to provide an exemplary healthcare service. The Trust is committed to promoting equality and diversity best practice both within the workforce and in any other area where it has influence.

8.3 The Trust will therefore take every possible step to ensure that this procedure is applied fairly to all employees regardless of race, ethnic or national origin, colour or nationality; gender (including marital status); age; disability; sexual orientation; religion or belief; length of service, whether full or part-time or employed under a permanent or a fixed-term contract or any other irrelevant factor.

8.4 Where there are barriers to understanding e.g. an employee has difficulty in reading or writing or where English is not their first language additional support will be put in place wherever necessary to ensure that the process to be followed is understood and that the employee is not disadvantaged at any stage in the procedure. Further information on the support available can be sought from the Human Resource Department.

9. Monitoring & Review

9.1 The Information Governance Steering Group (IGSG) will be responsible for the monitoring the policy and its supporting processes and documentation, reporting regularly to the Trust IM&T Control Board.

9.2 This policy will be in place for three years. Any changes to legislation, statute or NHS operational guidance which requires a change of policy within the three year period will be considered by the IGSG.

9.3 In the event of significant failure of this policy, then the group will approve temporary changes prior to formal review.

10. Contacts & Further Information

Caldicott Guardian
Helen Young, Director of Patient Care & Service Transformation
Helen.young@scas.nhs.uk

Head of Information Security & Governance
Mark Northcott
Mark.northcott@scas.nhs.uk

Information Governance Manager & DPO
Barbara Sansom
Barbara.sansom@scas.nhs.uk