South Central Ambulance Service
NHS Foundation Trust

CORPORATE POLICY & PROCEDURE NO:

SAFE HAVEN POLICY

December 2014

Author: Barbara Sansom Information Governance Manager	**Consultation & Approval** Staff Consultation N/A (no content change) Audit Committee: January 2015 Board Ratification: n/a
Equality Impact Assessment	December 2014 – Stage 1 Assessment undertaken – no issues identified
	Notification of Policy Release: All Recipient email – Staff Notice Boards (2 weeks) – Intranet -
Date of Issue:	December 2014
Next Review:	September 2018
Version:	4.3 amend Caldicott Guardian contact 4.2 no content changes – period extended to 30th Sept 2018 to allow for review under DPA 2018/GDPR 4.1 no content changes – period extended to 30th June 2018 to allow for review under new DPA / GDPR rules 4 (no content changes)

Contents

1.0 Introduction

1.1 All NHS organizations 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 organization, especially concerning sensitive information

1.2 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.

2.0 The scope of this policy

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

3.0 Equality Statement

3.1 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.

3.2. 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.

3.3. 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.

3.4. 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

4.0 Legislation and guidance

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

4.2 **Data Protection Act 1998**
(Principle 7): "*Appropriate technical and organizational measures shall be taken to make personal data secure"*

4.3 **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"*

5.0 Definitions

5.1 **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.

5.3 **Personal Information**
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.

5.4 **Sensitive personal information**
Sensitive personal information is where the personal information contains details of that person's:

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

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

6.0 Where safe haven procedures should be in place

Safe haven procedures should be in place in any location where large amounts of personal information is being received, held or communicated especially where the personal information is of a sensitive nature. There should be at least one area designated as a safe haven at each of the Trust sites.

7.0 Responsibilities for Implementing the Safe Haven Policy

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

7.2 **Information Governance Manager**
The Information Governance Manager is responsible for coordinating improvements in: data protection, the confidentiality code of conduct and with the Director of IM&T on information security.

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

8.0 Requirements for safe havens

8.1 Location/security arrangements

- It 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 member of staff who work in the same building or office, or any visitors.
- If 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, 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 have a secure screen saver function and be switched off when not in use.
- Equipment such as fax machines in the safe haven should have a code password and be turned off out of office hours.

8.2 Fax machines

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. 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.
- You notify the recipient when you are sending the fax and ask them to acknowledge receipt.
- Care is taken in dialing the correct number and wherever possible, programme numbers into machines to prevent misdialling
- Confidential faxes are not 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

8.3 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 marked private and confidential

8.4 Computers

- Access to any PC must be password protected, this must not be 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 have 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 password protected
- Clinical information must be clearly marked

- Emails must be sent to the right people, check and double check 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"
- 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 Trusts Email policy and Confidentiality Policy for more guidance on sending of personal information electronically.

9.0 Sharing information with other Organizations (Non NHS)

9.1 Employees of the Trust authorised to disclose information to other organisations outside the NHS must seek an assurance that these organisations have a designated safe haven point for receiving personal 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 requirements:

- Data Protection Act 1998
- Common Law Duty of Confidence
- NHS Code of Practice: Confidentiality

9.2 Staff sharing personal information with other agencies should be aware of protocol agreements made with other agencies, for example Police Forces, Social Services

10.0 Other relevant polices

Other policies that need to be read in conjunction with this policy are:

- **Records management and Lifecycle Policy**
  Storage, handling, retention and destruction of records
- **Confidentiality code of conduct**
  Rules for the use, access to, and disclosure of records
- **Email Policy**
  Guidance on content
- **Information Sharing Protocol**

All of these documents are available on the Trust Internet and Intranet pages.

11.0 Contacts and further information

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

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