South Central Ambulance Service
NHS Foundation Trust

# CORPORATE POLICY & PROCEDURE NO. 10

# DATA PROTECTION POLICY

# JUNE 2018

| DOCUMENT INFORMATION | |
|---|---|
| **Author:**<br>Barbara Sansom,<br>Information Governance Manager | **Consultation & Approval**<br>Staff Consultation 21 days<br>Audit Committee: 10th September 2018<br>Board Ratification: N/A |
| **Equality Impact Assessment** | April 2018 – Initial/High Level Assessment undertaken – no issues identified |
| **Data Protection Impact Assessment:** | April 2018 - Stage 1 Assessment undertaken – no issues identified |
| **Notification of Policy Release:** | Notification of Policy Release:<br>All Recipient email Intranet<br>Website |
| **Date of Issue:** | June 2018 |
| **Next Review:** | June 2021 |
| **Version:** | **7.0** – content changes to reflect General Data Protection Regulations (GDPR) & Data Protection Act (DPA) 2018<br>6.1 no content changes – period extended to 30th June 2018 to allow for review under new DPA / GDPR rules<br>6 (no content changes) |

**CONTENTS**

# 1. Introduction

## 1.1. The need for a Data Protection policy

The South Central Ambulance Service (SCAS) NHS Foundation Trust needs to process (collect, use, retain, protect, disclose and delete) personal data about people to carry out its business activities and fulfil its statutory responsibilities as an ambulance service.

The personal data it processes relates to past, current, and prospective patients, employees, clients/customers, suppliers, and others with whom it communicates. Some processing is carried out to satisfy legal obligations.

No matter the method, reasons or format of processing, data must be handled appropriately and the rights and freedoms of individuals must be protected.

This policy details how the Trust will comply with the all relevant UK and European legislation as well as meet the standards for data protection set by the NHS.

### 1.1.1. Personal Data

Personal data means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

### 1.1.2. Sensitive Personal Data

Sensitive data also referred to as special categories of personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data (where used for ID purposes), data concerning health or data concerning an individual's sex life or sexual orientation.

## 1.2. Aim

The South Central Ambulance Service NHS Foundation Trust's data protection policy aims to ensure that:

- Data protection by design is incorporated into administrative procedures where these involve the processing of personal data.
- There is clear definition of responsibilities across the Trust for complying data protection legislation.
- Anyone managing and handling personal information;
    - Is appropriately trained to do so
    - Understands their legal and contractual responsibilities for complying with data protection legislation
    - Is appropriately supervised and supported
- Clear procedures on handling personal information are in place
- Anyone wanting to make enquiries about handling personal information knows what to do
- Subject rights requests and requests for information are processed with a co-ordinated approach.
- A mechanism is in place for investigating and reporting data breaches / near misses / incidents
- Procedures for handling personal information are regularly assessed and evaluated

### 1.3. Key References

#### 1.3.1. Legislation

- Public Records Act 1967
- Police and Criminal Evidence Act 1984
- Access to Medical Reports Act 1988
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Crime & Disorder Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Privacy and Electronic Communications Regulations 2003
- Childrens Act 2004
- Environmental Information Regulations 2004
- Health and Social Care Act 2012
- General Data Protection Regulation 2018 (GDPR)
- Data Protection Act 2018

#### 1.3.2. Health and Social Service Guidance

- Ensuring Security and Confidentiality in NHS Organisations. (E5498).
- The Records Management: NHS Code of Practice
- Health Service Circular (HSC 2000/009) - Protection and Use of Patient Information
- Health Service Guidance (HSG (96) 18) - The Protection and
- Use of Patient Information
- Caldicott Report 1997 & Review of 2013

### 1.4. Principles

SCAS fully supports and complies with the key principles of the GDPR and DPA 2018. In summary, they require that personal data is:

- Processed lawfully, fairly and in a transparent manner.
- Processed to limited, stated and specific purposes. It should not be disclosed in an incompatible manner.
- Adequate, relevant and limited to what is necessary.
- Accurate and up to date.
- Not kept for longer than is necessary for the purpose of processing; and
- Kept safe and secure.
- In addition, we are required to demonstrate how we have complied with these principles.

## 2. Scope

This policy 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. Roles and Responsibilities

### 3.1. The Chief Executive

The Chief Executive is the Trust's Accountable Officer and has ultimate responsibility for data protection, ensuring that risks are assessed and mitigated to an acceptable level.

The Accounting Officer is responsible for the Information Governance Assurance Statement that confirms the Trust meets the information governance standards in respect of data security set out in Department of Health guidance.

### 3.2. Information Governance Steering Group (IGSG)

The Information Governance Steering Group has membership drawn from all departments and directorates to ensure that data protection and information governance is embedded within the organisational structure. The responsibilities of the IGSG include:

- monitoring compliance with legislation and Trust's policies
- identifying risks and mitigating to an acceptable level
- agreeing data protection policy

### 3.3. Senior Information Risk Owner (SIRO)

The SIRO for the Trust is the Director of Finance. The role is accountable for the overall development and maintenance of data protection and information governance within the Trust. The SIRO acts as champion for information risk on the Board of Directors and advises on the effectiveness of risk management across the Trust.

### 3.4. Caldicott Guardian

The Trust's Caldicott Guardian is the Executive Director of Patient Care.

The Caldicott Guardian serves in an advisory role and is the conscience of the organisation. The

Caldicott Guardian has overall responsibility for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.

### 3.5. 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.

### 3.6. The Information Governance Manager

The Information Governance Manager is the lead senior manager responsible for ensuring the Trust complies with all aspects of data protection and information governance. The role is responsible for completing the Data Security Toolkit as well as setting and implementing appropriate policies and procedures.

### 3.7. Information Asset Owners

Information Asset Owners (IAOs) are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. In particular, they are responsible for:

- Completing and maintaining information system governance manuals which detail records or processing activity.
- Undertaking data protection impact assessments where appropriate.
- Ensuring that any data sharing is conducted in accordance with the Trust's guidelines.
- Policies and procedures are adopted and implemented as appropriate.
- Ensure that staff are aware of and comply with information governance and record management standards for the effective use of their information assets.

IAOs may be assigned ownership of several assets within the Trust.

### 3.8. Information Asset Administrators

Information Asset Administrators are operational members of staff who understand and are familiar with information risks in their area or department. They implement the organisation's data protection policy for those information assets they support and will provide assurance reports and support to the relevant Information Asset Owner as necessary.

### 3.9. Information Governance Team

The Information Governance Team provides support to the Information Governance Manager. The team ensures appropriate responses to all freedom of information and data subject requests within the allocated timescale, liaising with the appropriate professionals.

### 3.10. All Staff

All SCAS staff have a personal responsibility to process personal information in accordance with relevant legislation, this policy and any other policy or guidance issued by the Trust.

In particular, staff should:

- Complete relevant training as required.
- Promptly report any suspected breaches.
- Seek advice where they are unsure how to comply with data protection legislation or this policy.
- Respond promptly to requests from the Information Governance department in connection data subject rights and freedom of information requests.
- Understand that failure to comply with Trust policy is treated seriously and can lead to disciplinary action.
- Understand it is an offence for an individual, knowingly or recklessly, to unlawfully disclose personal data and can lead to personal prosecution by the Information Commissioner's Office.

## 4. Breaches of Data Protection Legislation

The Trust requires that all incidents involving a possible breach of data protection legislation be reported, documented and investigated. The Trust promotes a culture where incidents can be reported and investigated in a non-punitive and supportive environment to ensure the most appropriate action can be taken.

Depending on the nature and severity of the incident, it may be necessary to inform all individuals affected and the Information Commissioner's Office.

For guidance on reporting data protection breaches, refer to the Incident Reporting Policy (IM&T Policies – Section 2Z)

## 5. Linked Trust Documents

- Information Governance Policy
- Information Governance Strategy
- Confidentiality Policy
- Freedom of Information Policy
- IM & T Policies & Procedures
- Lifecycle Policy
- Safe Haven Policy

## 6. Equality

6.1. 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.

6.2. 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.

6.3. 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.

6.4. 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.

## 7. Monitoring & Review

7.1. The Information Governance Steering Group will be responsible for monitoring the policy and it's supporting processes and documentation, reporting regularly to the Trust IM&T Control Board in respect of any incidents and remedial actions taken. Reports on any data breaches will be routinely reported and escalated as appropriate to the Trusts IM&T Control Board, Audit Committee and Executive Group including details of findings and remedial action taken.

7.2. This policies 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 Information Governance Steering Group.

7.3. In the event of significant failure of any policy then the group will approve temporary changes prior to formal review.

7.4. The policy will next be reviewed in June 2021.