The Scottish Ambulance Service

DATA PROTECTION POLICY

Version 4.0

DOCUMENT CONTROL SHEET:

The Policy will be reviewed bi-annually and also updated when required taking into account any new legislation and the operational requirements of SAS.

Key Information:

Title:	Data Protection Policy
Date Published/Issued:	15/12/2022
Date Effective From:	15/12/2022
Version/Issue Number:	V4.00
Document Type:	Policy
Document status:	Approved
Author:	Information Governance Officer Head of Business Intelligence
Owner:	Senior Information Risk Owner
Approver:	Information Governance Group Policy Review Group Staff Governance Committee
Contact:	sas.infogov@nhs.scot
File Location:	SAS Intranet: Information Governance Policies and Procedures (sharepoint.com)

Revision History:

Version:	Date:	Summary of Changes:	Name:
1.00	Apr 2001	Approved version	RJ
2.00	May 2004	Approved version	RJ
3.00	Apr 2008	Approved version	RJ
4.00	Dec 2022	Approved version	KB

Approvals: This document requires the following signed approvals.

Name:	Date:	Version:
Information Governance Committee	01/12/2021	V3.04
Policy Review Group	11/10/2022	V3.05
Staff Governance Committee	15/12/2022	V3.05

Distribution: This document has been distributed to:

Name:	Date of Issue:	Version:
Information Governance Committee	01/12/2021	V3.04
Policy Review Group	10/05/2022	V3.04
Policy Review Group	11/10/2022	V3.05
Staff Governance Committee	15/12/2022	V3.05

Linked Documentation:

Document Title:
SAS Data Protection Impact Assessment and Guidance
SAS Information Governance Policy
SAS Information Security Incident Reporting and Management Procedure
SAS Information Security Policy

Equality and Diversity Impact Assessment:

15/11/2021 – No equality and diversity impacts identified

1. INTRODUCTION

The Scottish Ambulance Service is required to collect and use a variety of personal information about people in order to operate effectively as a health care provider.

Such people include but are not limited to patients, employees (present, past and prospective), suppliers and other business contacts. The data may include identifiers such as name, address, email address, data of birth, CHI Number, National Insurance Number. It may also include private and confidential information, and special categories of personal data.

All personal information, irrespective of how it is collected, recorded and used must be dealt with appropriately to ensure compliance with data protection legislation – the UK General Data Protection Regulation (GDPR) tailored by the Data Protection Act 2018 (DPA2018).

The Scottish Ambulance Service has registered the purposes for which it collects personal information with the Information Commissioner's Office.

2. SCOPE

This policy applies to all staff employed by the Service, Contractors, Agency Staff, Volunteers and third party suppliers.

All staff must meet the standards of practice outlined in this document as well as those included within their terms of employment. Those who are registered healthcare professionals must also keep to their own regulatory organisation's standards of conduct and practice.

3. DEFINITIONS

The UK GDPR applies to controllers and processors.

- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.

The UK GDPR applies to the processing of personal data, this covers information about any natural person who:

- Can be identified or who are identifiable, directly from the information in question; or
- Can be indirectly identified from that information in combination with other information.

Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.

Personal data can also include special categories of personal data or criminal conviction and offences data. The processing of this information is subject to tighter controls and can only be used in more limited circumstances.

Special category data is defined as information relating to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Health data
- Sexual history and/or sexual orientation

4. THE DATA PROTECTION PRINCIPLES

The Service fully endorses and adheres to the Principles of Data Protection as set out in the UK GDPR, namely that:

Principle 1: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes.

Principle 3: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Principle 4: Personal data shall be accurate and, where necessary, kept up to date.

Principle 5: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Principle 6: Personal data shall be 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.

Principle 7: The controller shall be responsible for and be able to demonstrate compliance with the above principles.

5. ROLES AND RESPONSIBILITIES

5.1. Chief Executive

The Chief Executive has overall accountability for The Service's compliance with data protection law, the common law duty of confidentiality and associated regulation.

5.2. Information Governance Group (IGG)

The SAS Information Governance Group, an Audit Committee sub-group, monitors the compliance of SAS with its data protection obligations, along with the other information governance regulatory and policy obligations that are monitored as part of its remit.

5.3. Senior Information Risk Owner (SIRO)

The SIRO ensures that SAS information assets and risks are managed such that data protection compliance obligations are considered appropriately.

5.4. Information Asset Owners (IAOs)

Information Asset Owners, identified in our Information Asset Register (IAR), ensure that those information assets which comprise personal data for which they are responsible are managed in compliance with data protection law.

5.5. Data Protection Officer (DPO)

The Data Protection Officer (DPO) has specific responsibility for:

- Informing and advising the Service and its staff about their obligations to comply with data protection law
- Monitoring compliance with data protection law
- Being the first point of contact for the Information Commissioner's Office (ICO) and people whose personal data are processed by the Service.

5.6. Line Managers

Managers at all levels are responsible for ensuring they understand this Policy and that the staff for whom they are responsible are aware of, understand and adhere to it.

They are also responsible for ensuring staff are updated and supported in regard to understanding and implementing any changes in this policy.

5.7. All Staff

All staff who work for or under contract to the Service, including contractors, students, agency, bank staff and volunteers are responsible for ensuring that they are aware of and understand the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis, seeking support when necessary.

All staff have a duty to report any suspected or actual adverse events associated with the processing of personal data, as specified in the SAS Information Security Incident Management Procedure.

Breaches of this policy, and therefore data protection law, may lead to disciplinary action, in line with the NHS Scotland Workforce Conduct Policy

6. POLICY FRAMEWORK

The Scottish Ambulance Service (the Service) will:

- Ensure that an appropriate framework is in place encompassing relevant roles within the organisation that have responsibility for data protection, including the Data Protection Officer and Head of Information Governance, the Senior Information Risk Owner, Information Asset Owners and Caldicott Guardian.
- Provide training for all staff members who handle personal information and ensure access to further guidance and support

- Carry out regular checks to monitor and assess new processing of personal data and to ensure the Service notification to the Information Commissioner is updated to take account of any changes in processing of personal data
- Develop and maintain procedures to ensure compliance with data protection legislation, to cover for example:
    - data protection impact assessments
    - managing responses to subjects' rights requests
    - management of personal data breaches
    - provision of privacy information
    - training and compliance testing
- Maintain a record of processing activities
- Ensure the organisation complies with its transparency and fair processing obligations in relation to data subjects' personal data

7. MONITORING

Compliance with this document will be monitored via the Information Governance Group, together with independent reviews by Internal Audit on a periodic basis.

The Head Information Governance is responsible for the monitoring, revision and updating of this document on a two yearly basis or sooner if the need arises.