The Scottish Ambulance Service

INFORMATION GOVERNANCE POLICY

Version 3.00

DOCUMENT CONTROL SHEET:

The procedure 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:	Information Governance Policy
Date Published/Issued:	15/12/2022
Date Effective From:	15/12/2022
Version/Issue Number:	V3.00
Document Type:	Policy
Document Status:	Approved
Author:	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:**
1.01	01/12/2009	Approved version	RJ
2.00	10/05/2018	Approved version	KB
3.00	15/12/2022	Approved version	KB

Approvals: This document requires the following signed approvals.

Name:	**Date:**	**Version:**
Information Governance Group	02/09/2021	2.01
Policy Review Group	10/05/2022	2.01
Policy Review Group	11/10/2022	2.02
Staff Governance Committee	15/12/2022	2.02

Distribution: This document has been distributed to

Name:	**Date of Issue:**	**Version:**
Information Governance Group	02/09/2021	2.01
Policy Review Group	10/05/2022	2.01
Policy Review Group	11/10/2022	2.02
Staff Governance Committee	15/12/2022	2.02

Linked Documentation:

Document Title:
SAS Data Protection Policy
SAS Document Security Classification Policy
SAS Documents Storage, Disposal and Retention Policy
SAS Forensic Readiness Policy
SAS Freedom of Information Policy
SAS ICT Security Policy
SAS Information Security Policy
SAS Records Management Policy
SAS Social Media Policy
SAS Information Security Incident Management Procedure
UK Caldicott Guardian Council website
Guidance for Information Asset Owners and Information Champions

Equality and Diversity Impact Assessment:

28/06/2021 – No equality and diversity impacts identified

1. INTRODUCTION

1.1. Background

Information Governance is the term used to describe the legal framework, which regulates how information is processed (e.g. obtained, handled, managed and disclosed).

The Scottish Ambulance Service (the Service) recognises that information plays a key part in supporting all areas of the Service. It also acknowledges that all information (including, but not only, information relating to and identifying individuals) must be dealt with legally, securely, efficiently and effectively, in order to deliver the best possible services.

Information Governance has four fundamental aims:

- To support the provision of high quality care by promoting the effective and appropriate use of information.
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources.
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards.
- To enable organisations to understand their own performance and manage improvement in a systematic and effective way.

1.2. Aim

This policy will establish the Service’s policy framework in relation to Information Governance (IG) by establishing and maintaining sub-policies and procedures to ensure compliance with the requirements of the law and expectations of all whose data we hold.

The Service will seek to develop and maintain an Information Governance culture whereby its staff and others working on its behalf understand the importance of Information Governance, know their responsibilities, and manage information appropriately.

2. SCOPE

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

This policy is developed to complement and comply with relevant data protection, records management and freedom of information legislation.

3. ROLES AND RESPONSIBILITIES

3.1. Scottish Ambulance Service Board

The **Scottish Ambulance Service Board** has accountability for ensuring that Service has an Information Governance Policy and that adequate controls, assurance and governance are in place.

3.2. Information Governance Group

The **Information Governance Group** is accountable to the **Audit Committee** via the Chairperson who will be an Executive Director. The objective of the Information Governance Group is to ensure that a robust framework is in place that meets the requirements and standards that apply to the handling of information.

3.3. Chief Executive

The **Chief Executive** is the Accountable Officer with overall responsibility for Information Governance. This responsibility is delegated to the respective Senior Information Risk Owner (SIRO).

3.4. Senior Information Risk Owner (SIRO)

The **SIRO** is responsible for implementing and leading the Information Governance (IG) risk assessment and management processes within the Service and to advise the Board on the effectiveness of information risk management across the Service. They are the chair of the Information Governance Group.

The role of SIRO relies on Information Asset Owners (IAO) to manage information risks at an operational and system level, these roles are described in Guidance for Information Asset Owners and Information Champions.

3.5. Caldicott Guardian

The Service's Medical Director has been appointed the **Caldicott Guardian.** They are responsible for facilitating the understanding and awareness of individual and Service-wide responsibilities for maintaining the governance of patient identifiable information in line with the Caldicott Principles. Further information about these principles can be found on the UK Caldicott Guardian Council website.

3.6. Data Protection Officer (DPO)

The **DPO** is the Head of Business Intelligence who reports to the SIRO, but can also act independently of the SIRO and report directly to the Board about data protection matters. These may include information governance risks to the organisation, privacy concerns or recommendations with regard to potential changes to, or new initiatives that, involve processing of personal data.

The DPO is responsible for providing advice and monitoring compliance with Data Protection Legislation and is the first point of contact in the Service for data protection matters. They are also the first point of contact for the Information Commissioner's Office (ICO).

3.7. Information Asset Owners (IAO)

The Service's **Information Asset Owners (IAOs)** are responsible for ensuring that risk assessments are carried out and appropriate security measures are in place to protect the information they are accountable for.

3.8. Head of Information Governance

The Head of Business Intelligence carries out the role of Head of Information Governance. In conjunction with members of the Information Governance Committee they will be responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the Scottish Ambulance Service and for the raising of its profile.

3.9. General Manager ICT

The General Manager ICT Technology is responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure the Service's systems and infrastructure remain compliant with data protection legislation. They are responsible for ensuring that all the Service's electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

3.10. Line Managers

Managers within the Scottish Ambulance Service are responsible for ensuring that this Policy and any supporting Policies, Standards and Guidelines are built into local processes and that there is on-going compliance.

3.11. All Staff

All staff, whether permanent, temporary or contracted as well as volunteers and contractors are responsible for ensuring that they are aware of the information governance requirements of their role and for ensuring that they comply with these requirements on a day to day basis.

All staff are mandated to undertake mandatory information governance training in line with the training needs analysis programme as agreed by the Information Governance Group. Information governance training is required to be undertaken by all staff within the required timescales.

4. POLICY FRAMEWORK

The Scottish Ambulance Service has developed a framework to support this Information Governance Policy. This consists of a set of Information Governance policies, related procedures and guidance to cover all aspects of Information Governance.

Associated Information Governance Policies include:

Data Protection Policy This policy sets out the roles and responsibilities for compliance with data protection legislation.

Document Security Classification Policy This policy outlines how documents may be classified for security, protection and management of information in line with relevant legislation and records management standards.

Document Storage, Retention and Disposal Policy This policy sets the context of record keeping within SAS and discuss the obligations of the Service to create, store, maintain, review, and dispose of records appropriately.

Forensic Readiness Policy This policy provides a systematic, standardised and legal basis for the preservation of digital evidence that may be required from a formal dispute or legal process.

Freedom of Information Policy This policy sets out the roles and responsibilities for compliance with the Freedom of Information Act and Environmental Information Regulations.

ICT Security Policy This policy outlines the security of ICT systems in use at all Service sites and while mobile devices are off-site.

Information Security Policy This policy is to protect, to a consistently high standard, all information assets. The policy defines security measures applied through technology and encompasses the expected behaviour of those who manage information within the organisation

Records Management Policy This policy is to promote the effective management and use of information, recognising its value and importance as a resource for the delivery of corporate and service objectives.

Social Media Policy This policy provides a structured approach to using social media and will ensure that it is effective, lawful and does not compromise Scottish Ambulance Service information, ICT or reputation.

5. INFORMATION GOVERNANCE GROUP

The Scottish Ambulance Service has established an Information Governance Group to ensure that a robust framework is in place that meets the requirements and standards that apply to the handling of information. The Group reports quarterly to the Scottish Ambulance Service Audit Committee.

6. INFORMATION GOVENRANCE TEAM

The Information Governance Team will provide expert advice and guidance to all staff on all elements of Information Governance. The team is responsible for:

- Providing advice and guidance on internal Information Governance to all staff
- Providing support advice and guidance to internal strategic projects and programmes
- Investigate internal information security incidents in line with the SAS Information Security Incident Management Procedure
- Liaison with strategic external stakeholders such as the Scottish Government eHealth Department, the ICO (UK) and the Scottish Information Commissioner
- Identifying key strategic IG issues and lead work to analyse problems, find solutions and communicate outcomes
- Working with directorates and departments to ensure there is consistency of IG across the organisation
- Developing internal IG policies and procedures
- Working with thirds parties to establish protocols on how to share information
- Developing IG awareness and training programmes for staff
- Ensuring compliance with Data Protection, Information Security and other information related legislation
- Handle and respond to freedom of information requests on behalf of the Organisation
- Providing support to the Caldicott Guardian and Senior Information Risk Owner (SIRO) for internal Information Governance related issues
- Working with external stakeholders to ensure consistency of information governance standards and requirements across the NHS in Scotland

7. MONITORING

Compliance with the policies and procedures laid down in this document will be monitored by the Information Governance Team, together with independent reviews by both Internal and External Audit on a periodic basis.