APPROVED VERSION 2.00

The Scottish Ambulance Service

INFORMATION GOVERNANCE POLICY

Version 2.00

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:	10th May 2018
Date Effective From:	10th May 2018
Date of Review:	10th May 2020
Version/Issue Number:	V2.00
Document Type:	Policy
Document Status:	Approved
Author:	Katy Barclay, Information Services & Governance Manager
Owner:	Dr Patricia O'Connor, Director of Care Quality and Strategic Development
Approver:	Policy Review Group Staff Governance Committee National Partnership Forum
Contact:	Katy Barclay, Information Services & Governance Manager
File Location:	@SAS

Revision History:

Version:	Date:	Summary of Changes:	Name:
1.01	Dec 2009	Approved version	RJ
2.00	10 May 2018	Approved version	KB

Approvals: This document requires the following signed approvals.

Name:	Date:	Version:
Policy Review Group	Oct 2017	1.03
National Partnership Forum	Nov 2017	1.03
Partnership Representatives	Mar 2018	1.04
Staff Governance Committee	Apr 2018	1.04

Distribution: This document has been distributed to

Name:	Date of Issue:	Version:
Policy Review Group	May 2017	1.02
National Partnership Forum	Nov 2017	1.03
Partnership Representatives	Mar 2018	1.04
Staff Governance Committee	Apr 2018	1.04

Linked Documentation:

Document Title:
SAS Information Security Policy
SAS Information Security Incident Management Procedure
SAS Internet and Email Policy
SAS Laptop Security Policy
SAS Data Protection Policy
SAS Information Asset Policy (under development)
SAS Data Transfer & Backup of Personal Information Policy
SAS Homeworking Policy
SAS Records Management Policy
SAS Documents Storage, Disposal and Retention Policy

Equality and Diversity Impact Assessment:

15 March 2018 – No equality and diversity impacts identified

1. INTRODUCTION

1.1. The Scottish Ambulance Service (the Service) recognises that information plays a key part in supporting clinical governance, service planning and performance management. It also acknowledges that personal information relating to patients, the public and staff must be dealt with legally, securely, efficiently and effectively, in order to deliver the best possible services. This policy will establish and maintain sub-policies and procedures to ensure compliance with the requirements of the Information Governance Toolkit, the law and expectations of all whose data we hold.

1.2. The Service further recognises the need for an appropriate balance between openness and confidentiality in the management and use of information and fully supports the principles of information governance. While accepting its public accountability, it also acknowledges that equal importance must be placed on confidentiality and security arrangements in order to safeguard, both personal information about patients and staff and commercially sensitive information. At the same time there is the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the individual patient and, in some circumstances, the wider public interest. It is essential that accurate, timely and relevant information is recorded. This is essential to deliver the highest quality health care. As such it is the responsibility of all staff to promote data quality and confidentiality. The 4 key areas which this policy brings together are openness, information quality, information security and legal compliance

2. SCOPE AND DEFINTIONS

2.1. 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.

2.2. Information Governance covers the following topics:

- Information Governance Policy and Planning
- General Data Protection Regulation (from 28th May 2018)
- Data Protection Act 1998
- Confidentiality
- Caldicott - Clinical Information
- Freedom of Information (Scotland) Act 2002
- Information Management
- Information Security
- Health Records
- Administrative Records
- Information Quality Assurance

3. OPENNESS

3.1. Non-confidential information held by the Scottish Ambulance Service and its services should be available to the public through a variety of media.

3.2. The Scottish Ambulance Service will establish and maintain policies to ensure compliance with the Freedom of Information (Scotland) Act 2002.

3.3. Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients.

3.4. The Scottish Ambulance Service will have clear procedures and arrangements for liaison with the press and broadcasting media.

3.5. The Scottish Ambulance Service will produce and maintain an up to date Information Asset Register that will be available via its website.

3.6. The Scottish Ambulance Service will have clear procedures and arrangements for handling queries and/or requests for information from patients and the public.

4. INFORMATION QUALITY

4.1. The Scottish Ambulance Service will establish and maintain policies and procedures for information quality assurance and the effective management of records.

4.2. The Scottish Ambulance Service will undertake or commission annual assessments and audits of its information quality and records management arrangements.

4.3. Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

4.4. Wherever possible, information quality will be assured at the point of Collection.

4.5. Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

4.6. The Scottish Ambulance Service will promote information quality and effective records management through policies, procedures/user manuals and training.

4.7. Process will be in place to ensure that anyone adding or amending clinical information, opinions or patient management decisions can be subsequently identified.

5. INFORMATION SECURITY

5.1. The Scottish Ambulance Service will establish and maintain policies for the effective and secure management of its information assets and resources.

5.2. The Scottish Ambulance Service will undertake regular assessments and audits of its information and IT security arrangements through formal internal and/or external annual planned audit processes.

5.3. The Scottish Ambulance Service will promote effective confidentiality and security practice to its staff through policies, procedures and training.

5.4. The Scottish Ambulance Service will maintain and review incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

5.5. The Scottish Ambulance Service will regard all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

6. LEGAL COMPLIANCE

6.1. The Scottish Ambulance Service regards all identifiable personal information relating to patients and staff as confidential and will ensure that the handling of such information complies with the Data Protection Act 1998 and the General Data Protection Regulation - except where there are legitimate exemptions to be applied and/or there is a legal requirement to override the requirements of the Act.

6.2. The Scottish Ambulance Service will undertake or commission regular assessments and audits of its compliance with legal requirements.

6.3. The Scottish Ambulance Service will establish and maintain policies to ensure compliance with the Data Protection Act 1998, the General Data Protection Regulation, The Human Rights Act 1998, the Public Records (Scotland) Act 2011, Common Law of confidentiality and the Freedom of Information (Scotland) Act 2002.

6.4. The Scottish Ambulance Service will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Adult and Child Protection law).

7. ROLES AND RESPONSIBILITIES

7.1. 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.

7.2. 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.

7.3. 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.

7.4. All staff, whether permanent, temporary or contracted should receive induction training on Information Governance issues and top–up training as required.

7.5. Information Governance performance will be monitored by the Information Governance Group and any audit results, once approved by the committee, will be submitted within a quarterly report to the Audit Committee.

8. SPECIFIC ROLES

8.1. The Chief Executive is the Accountable Officer with overall responsibility for Information Governance – especially information Security (as mandated by the Scottish Government Health Department).

8.2. The Director of Care Quality and Strategic Development is currently mandated to lead and implement Information Governance and is Chairperson of the Information Governance Committee.

8.3. Compliance with Data Protection is delegated to individual members of staff, contractors or volunteers who handle personal data of any kind. Responsibility for overseeing and auditing day to day compliance rests with the Information Services and Governance Manager.

8.4. Compliance with The Freedom Of Information (Scotland) Act 2002 rests within the Corporate Affairs function and responsibility for overseeing and auditing day to day compliance rests with the Head of Corporate Affairs and Engagement.

8.5. Responsibility for Information Security and the development of Information Systems rests with the General Manager, Communications and ICT, along with Network Security and ICT system specialists.

8.6. The Information Services and Governance Manager, in conjunction with members of the Information Governance Committee 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

9. RISK MANAGEMENT & BUSINESS CONTINUITY

9.1. Information Asset Owners will carry out a risk assessment for their information and record systems to ensure that suitable disaster recovery and contingency capabilities are implemented. In rare circumstances, the Chief Executive may approve the operation of an information system without recovery and contingency facilities where the risk assessment justifies this.

9.2. Recovery procedures will be developed for all operational systems and where relevant an appropriate contingency plan must also be prepared to ensure an acceptable level of service and control is maintained following system failure.

9.3. All recovery and contingency plans will be kept up to date with system changes. The Service will test these arrangements initially and at intervals thereafter as part of its ongoing Information Security management programme.