Southern Health and Social Care Trust

Information Governance Policy

Lead Policy Author & Job Title:	Catherine Weaver – Head of Information Governance
Directorate responsible for document:	**Performance & Reform**
Issue Date:	
Review Date:	**March 2025**

Policy Checklist

Policy name:	Information Governance Policy
Lead Policy Author & Job Title:	Catherine Weaver – Head of Information Governance
Director responsible for Policy:	Lesley Leeman
Directorate responsible for Policy:	**Performance & Reform**
Equality Screened by:	Catherine Weaver
Trade Union consultation?	Yes ☒No ☐
Policy Implementation Plan included?	Yes ☒ No ☐
Date approved by Policy Scrutiny Committee:	TBC
Date approved by SMT:	
Policy circulated to:	Directors and Information Governance Committee
Policy uploaded to:	Sharepoint

Version Control

Version:	Information Governance Policy Version 1.5
Supersedes:	Information Governance Policy Version 1.4

Version History

Version	Notes on revisions/modifications and who document was circulated or presented to	Date	Lead Policy Author
V1.3	Amendments to include GDPR	09012019	Head of Information Governance
V1.4	Update on Terminology including Cyber Security Manager and	02/03/2021	Head of Information Governance
V1.5	Updated Policy Template, change of Information Governance Forum to Digital Governance Steering Group. Addition of the Director for HROD as a PDG. Change in DPO role to Assistant Director of Informatics & Update on CIO roles.	09/01/2023	Head of Information Governance

Contents

1. INTRODUCTION

Information is a vital asset, both in terms of the clinical management of patients and the efficient management of services and resources. It plays a key part in corporate governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

1.1 PURPOSE

The purpose of this document is to provide guidance to all Health & Social Care (HSC) Trust staff on Information Governance compliance. Information Governance sets out the protocol for handling information in a confidential and secure manner to appropriate ethical and quality standards within the HSC.

The aim of this document is:

- To maximise the value of the Trust assets by ensuring that data is:
    - held securely and confidentially;
    - obtained fairly and lawfully;
    - recorded accurately and reliably;
    - used effectively and ethically; and
    - shared and disclosed appropriately and lawfully.

2. SCOPE OF POLICY

This policy applies to all individuals, whether employed or contracted to work for the Southern Health and Social Care Trust (the Trust) including:

- bank/agency/temporary;
- volunteer;
- student;
- secondee; and
- contractors (including Consultants and Field Experts (working in or on behalf of the Trust)

Reference to “information governance” in this document shall also mean reference to the following areas:

- Access to information (Freedom of Information Act 2000 and Subject Access Requests and Environmental Information Regulations);
- Data Protection Act 2018;
- Information Security assurance;
- Data Quality assurance;

- Secondary Use Assurance;
- Records Management compliance; and
- Confidentiality and the common law Duty of Confidentiality.

This policy applies to all processing activities on information held in any format and type such as (but is not limited to):

- patient/client/service user information;
- staff and personnel information;
- organisation, business and operational information;
- research, audit and reporting information.

All staff, whether employed or contracted, should be aware of their individual responsibilities for the maintenance of confidentiality, data protection, information security management and data quality (as set out in the contract of employment). Failure to maintain confidentiality may lead to disciplinary action, up to and including dismissal. Staff should also be aware of the Code of Practice on Protecting the Confidentiality of Service User Information published by the Department of Health (NI)

3.0 ROLES AND RESPONSIBILITIES

3.1 THE TRUST

The Trust Board is responsible for ensuring that the information governance function is appropriately managed in a manner which complies with relevant legislation and standards and that an Information Governance Framework is in place. The Trust undertakes the role of the Data Controller.

3.2 THE CHIEF EXECUTIVE

The Chief Executive as the Accountable Officer has overall accountability and responsibility for Information Governance in the Trust and is required to provide assurance through the Statement of Internal Control that all risks, including those relating to information, are effectively managed and mitigated.

3.3 PERSONAL DATA GUARDIAN

The Medical Director, the Director of Children's and Young People Services have been appointed as the Trust Personal Data Guardians (PDGs) for service user information and the Director of Human Resources and Organisational Development has been appointed as the Personal Data Guardian for Staff Information. The PDG:

- ensures that the Trust satisfies the highest practical standards for handling personal identifiable information;
- actively supports work to facilitate and enable information sharing, and advises on options for lawful and ethical processing of information as required;
- has a strategic role, which involves representing and championing information governance requirements and issues at Trust or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

3.4 THE SENIOR INFORMATION RISK OWNER

The Director of Performance and Reform is the Senior Information Risk Owner (SIRO). The SIRO has overall responsibility for managing information risk across the Trust and is the owner of the Information Asset Register. The SIRO is a member of the Senior Management Team and the Trust Board and provides written advice to the Accounting Officer on the content of the Statement of Internal Control in regard to information risk. See **Appendix B - Key Responsibilities of the Senior Information Risk Owner (SIRO)** for list of key responsibilities.

The SIRO is responsible to the Trust Board for ensuring that all Information risks are recorded and mitigated where applicable. The SIRO is responsible for ensuring that all record management issues (including electronic media) are managed in accordance with the Trust's Information Governance and Records Management Policies.

3.5 INFORMATION GOVERNANCE LEAD

The Assistant Director of Informatics leads on the Information Governance Programme and provides assurance to the SIRO and is also the Trust's Data Protection Officer.

3.6 HEAD OF INFORMATION GOVERNANCE

The Head of Information Governance is responsible for ensuring compliance on a day to day basis:

- to review and update Information Governance policy in line with local and national requirements;
- ensure that line managers are aware of the requirements of Information Governance and associated policies;
- monitor and report on compliance with Freedom of Information Act and Data Protection Act 2018;
- assess risk and advise on information incidents and data breaches to ensure consistent reporting to regulatory bodies;
- achieve compliance with the Information Management Controls Assurance Standard (IM CAS); and
- provide advice and guidance on Information Governance issues with targeted training as appropriate.

3.7 IT CYBER SECURITY MANAGER

The IT Cyber Security Manager is responsible for IT security within the Trust by

- providing advice on the design and implementation of IT security aspects of IT solutions;
- providing technical leadership on all aspects of the Trust's ICT security infrastructure ensuring Best Practice standards are adhered to;
- investigating ICT security breaches and incidents and where necessary reporting Network Security Systems breaches to the Competent Authority and;
- ensuring ICT security services operational documentation is up-to-date.

3.8 INFORMATION ASSET OWNER

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'.

The IAO role is to understand and assess risks to the information assets they 'own' and to provide assurance to the SIRO (via Head of Information Governance) on the security and use of those assets. They will ensure that all threats, vulnerabilities and impacts are properly assessed and included in their Directorate Risk Register and where necessary that these are escalated to the Corporate Risk Register by the Director.

See **Appendix C - Key Responsibilities of the IAO** - for a list of key responsibilities for Information Asset Owners.

3.9 ALL STAFF

It is the responsibility of each employee to adhere to this policy and all supporting Information Governance policies, procedures and guidance.

All staff members are required to undertake mandatory information governance e-learning modules. Information governance training is required to be undertaken on a three yearly basis.

All staff must ensure that they use the Trust's Information Technology systems appropriately, and adhere to the acceptable use of Information, Communication, Technology (ICT) Policy.

3.10 CHIEF ALLIED HEALTH PROFESSIONAL INFORMATION OFFICERs

The Chief Allied Health Professions Information Officer (CAHPIO) will provide strong professional support, leadership and advice to Directorates to develop, implement and establish structures to support the implementation of encompass safely and effectively. The CAHPIO will maintain a sustainable governance

framework for the review and development of evidenced based AHP content within the digital record.

3.11 DIGITAL GOVERNANCE STEERING GROUP

The Digital Governance Steering Group has responsibility for overseeing the implementation of the Information Governance Strategy, Information Governance Framework, and the Information Governance Policy. The Steering Group is also responsible for the annual Information Management Assurance Checklist (IMAC) assessment and oversees and monitors the implementation of the IMAC Action Plan.

4.0 KEY POLICY STATEMENT

4.1 DEFINITIONS

Information Governance is the framework of law and best practice that regulates the manner in which information (including information relating to and identifying individuals) is managed, i.e. obtained, handled, used and disclosed.

4.2 POLICY STATEMENT

The Trust's Information Governance Policy sets out a framework of Policies and Procedures, Standards and Guidance to cover all aspects of Information Governance which are aligned to the Trust's Information Governance Framework and the Regional Information Management Assurance Checklist. The Trust's performance is mandated by the Information Management Assurance Checklist Guidance (IMAC), is reported annually to the Department of Health (DoH) and forms a part of the Trust's assurance processes.

4.3 LEGISLATIVE COMPLIANCE, RELEVANT POLICIES, PROCEDURES AND GUIDANCE

Information Governance provides a consistent way for employees to deal with the many different information handling requirements.

The Trust, as the "legal person" and Data Controller for the purposes of the Data Protection Act 2018 will ensure that all personal data it holds is controlled and managed in accordance with the principles of the Data Protection Act 2018, the UK General Data Protection Regulations, European Convention of Human Rights (Article 8), Human Rights Act 1998 and common law Duty of Confidentiality. This is set out in the Trust's Data Protection Policy and Records Management Policy.

4.4 PRIVACY IMPACT ASSESSMENTS

For new service implementation or service change, the Project lead must liaise with the Head of Information Governance regarding the completion of a Data Protection Impact Assessment (DPIA). This assessment will consider privacy aspects and mitigate against any potential risk to personal/personal sensitive information.

4.5 INFORMATION GOVERNANCE DATA INCIDENTS

Head of Information Governance must be notified immediately of all information security incidents involving the unauthorised disclosure of personal identifiable data/information for consideration of any necessary actions.

A key function of the Digital Governance Steering Group is to monitor and review untoward occurrences and incidents relating to Information Governance and to ensure that effective remedial and preventative action is taken.

Information incident reporting is in line with the Trust's overall incident reporting processes.

5.0 IMPLEMENTATION & MONITORING OF THIS POLICY

The implementation of this Policy is evidenced and monitored through the agenda of the Information Governance Committee. The Information Governance Committee agenda and the Information Management Controls Assurance Standard action plan (IM CAS) encompass the objectives of this policy and Data Protection Act principles.

5.1 DISSEMINATION

This policy will be disseminated via the Policy Scrutiny Committee in line with Trust procedure. It is the responsibility of all Managers to ensure that staff have access to this policy.

5.2 RESOURCES TRAINING AND EDUCATION

All staff should receive basic information governance training appropriate to their role through either face to face training or an eLearning package on the Trust's eLearning platform.

Information Governance Training is incorporated into the Trust's Mandatory Training programme. It is a **mandatory** requirement for all staff in the Trust, without exception to undertake Data Protection training which is appropriate to their role. This includes staff on temporary contracts, secondments, agency staff, students and volunteers.

Different levels of training will be delivered:

- All staff to receive Information Governance awareness training as part of their corporate induction programme.

- Departmental induction must ensure that staff are made fully aware of all Information Governance policies and procedure.
- Practitioner level training e.g. SIRO (Senior Information Risk Owner), Personal Data Guardian, Information Asset Owners and Information Governance Team.

6.0 REVIEW AND MONITORING

This Policy will be reviewed in line with the Trust's Information Governance Strategy Incorporating Framework and monitoring process to ensure compliance with legislation and the requirements of the Information Management Controls Assurance Standard.

7.0 EVIDENCE BASE

- DHSSPS Information Management Controls Assurance Standard (2013);
- Southern Health & Social Care Trust Information Governance Strategy Incorporating Framework 2014/2015 – 2016/2017;
- IT Security Policy
- Records Management Policy
- Data Protection Act Policy
- Data Quality Policy

8.0 CONSULTATION PROCESS

The consultation process will be in line with the Trust's procedure for consultation on the introduction of new/revision of existing Trust policy.

9.0 EQUALITY STATEMENT

In line with duties under the equality legislation (Section 75 of the Northern Ireland Act 1998), Targeting Social Need Initiative, Disability discrimination and the Human Rights Act 1998, an initial screening exercise to ascertain if this policy should be subject to a full impact assessment has been carried out.

The outcome of the Equality screening for this policy is:

Major impact ☐

Minor impact ☐

No impact. ☒

10.0 ALTERNATIVE FORMATS

This document can be made available on request in alternative formats, e.g. plain English, Braille, disc, audiocassette and in other languages to meet the needs of those who are not fluent in English.

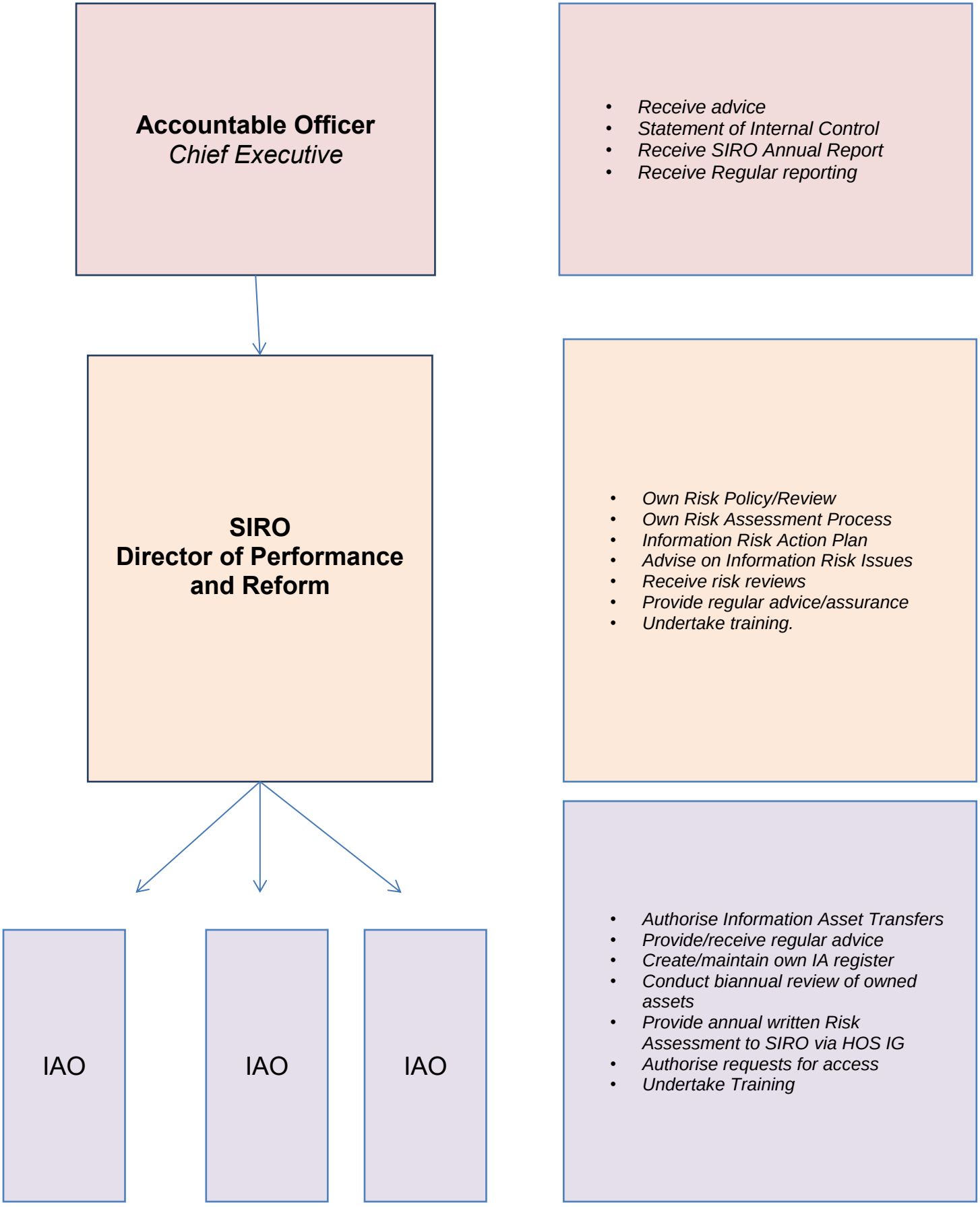
APPENDICES

Appendix A – Information Risk/Roles and Responsibilities

Appendix B – Key Responsibilities of the SIRO

Appendix C – Key Responsibilities of the IAO

Appendix A - Information Risk/Roles and Responsibilities



Appendix B - Key Responsibilities of the Senior Information Risk Owner (SIRO)

- To oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Strategy Incorporating Framework.

- To take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.

- To review and agree an action plan in respect of identified information risks via the Information Governance Forum.

- To ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.

- To provide a focal point for the resolution and/or discussion of information risk issues.

- To ensure the Board is adequately briefed on information risk issues.

- To advise the Chief Executive and the Trust Board on information risk management strategies and provide periodic reports and briefings on the Information Governance annual programme of work.

Appendix C - Key Responsibilities of the Information Asset Owners (IAO)

- To understand and address risks to the information assets they ‘own’ and provide assurance to the SIRO on the security and use of these assets (understands the Trust’s plans to achieve and monitor the right Information Governance culture across the Trust.
- IAO’s will take appropriate actions to:
    - Know what information they hold,
    - Know who has access to the information and why,
    - Ensure the confidentiality, integrity, and availability of all information that their system creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
    - Ensure that information assets are considered within the Directorate Risk Register assessment process on a quarterly basis
    - provide assurance to the SIRO on an annual basis in respect of security of information assets
    - Approve and oversee the disposal of information of the asset when no longer needed in line with ICT Procedure and or/the Trust Retention & Disposal Schedule.