### Policy Checklist

<table>
<thead>
<tr>
<th>Name of Policy:</th>
<th>Information Governance Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of Policy:</td>
<td>To provide guidance to all staff on their responsibilities regarding information governance and to ensure that the Trust is compliant with the Data Protection Act 1998 and other legislation and standards. To be read in conjunction with the Information Governance Strategy incorporating Framework 2014/2015 – 2016/2017.</td>
</tr>
<tr>
<td>Directorate responsible for Policy</td>
<td>Performance and Reform</td>
</tr>
</tbody>
</table>
| Name & Title of Author: | Claire Graham  
Head of Information Governance |
| Does this meet criteria of a Policy? | Yes |
| Staff side consultation? | Yes |
| Equality Screened by: | Claire Graham |
| Date Policy submitted to RM&PC: | 14 January 2015 |
| Policy Approved/Rejected/Amended | Comments received  
29 January 2015 |
<p>| Communication Plan required? | No |
| Training Plan required? | No |</p>
<table>
<thead>
<tr>
<th>Implementation Plan required?</th>
<th>Yes incorporated in Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any other comments:</td>
<td></td>
</tr>
<tr>
<td>Date presented to SMT</td>
<td></td>
</tr>
<tr>
<td>Director Responsible</td>
<td>Paula Clarke</td>
</tr>
<tr>
<td>SMT Approved/Rejected/Amended</td>
<td></td>
</tr>
<tr>
<td>SMT Comments</td>
<td></td>
</tr>
<tr>
<td>Date returned to Directorate</td>
<td></td>
</tr>
<tr>
<td>Lead for implementation</td>
<td></td>
</tr>
<tr>
<td>(Board Secretary)</td>
<td></td>
</tr>
<tr>
<td>Date received by Board</td>
<td>30 March 2015</td>
</tr>
<tr>
<td>Secretary (HQ) for database/</td>
<td></td>
</tr>
<tr>
<td>Intranet/Internet</td>
<td></td>
</tr>
<tr>
<td>Date for further review</td>
<td>2 year default</td>
</tr>
</tbody>
</table>
| **Title** | Title: Information Governance Policy  
Version: 0.5  
Reference number/document name: |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supersedes</strong></td>
<td>To support Information Governance Strategy incorporating Framework and to meet the requirements of the new Information Management Controls Assurance Standard</td>
</tr>
</tbody>
</table>
| **Originator** | Name of Author: Claire Graham  
Title: Head of Information Governance |
| **RM/Policy Committee & SMT approval** | Referred for approval by: Claire Graham  
Date of Referral:  
RM/Policy Committee Approval (Date) 14 Jan 2015 – tabled for comments  
Policy Scrutiny Committee approval 30 March 2015 |
| **Circulation** | Issue Date: January 2015  
Circulated By: Claire Graham  
Issued To: As per circulation List (Records Management Committee/Policy Scrutiny Committee) |
| **Review** | Review Date: January 2017  
Responsibility of (Name): Claire Graham  
Title: Head of Information Governance |
## CONTENTS

1.0 Introduction .................................................................................................................... 5

2.0 Scope of Policy ................................................................................................................. 5

3.0 Roles and Responsibilities .............................................................................................. 6

4.0 Key Policy Statement ....................................................................................................... 8

5.0 Implementation of this Policy ......................................................................................... 9

6.0 Review and Monitoring .................................................................................................. 10

7.0 Evidence Base ................................................................................................................ 10

8.0 Consultation Process ....................................................................................................... 10

Appendices .......................................................................................................................... 11
1.0 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.

2.0 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/Interner;
- secondee; and
- contractors (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);
- Data Protection Act 1998;
- Information Security assurance;
- Data Quality assurance;
- Secondary Use Assurance;
- Records Management compliance; and
• Confidentiality and the common law Duty of Care.

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. Failure to maintain confidentiality may lead to disciplinary action, up to and including dismissal.

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. 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 and the Director of Children’s and Young People Services have been appointed as the Trust Personal Data Guardians (PDGs). The PDG:

• ensures that the Trust satisfies the highest practical standards for handling person 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.

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 1998;
- 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 Security Manager

The IT 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;
- 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 **Information Governance Forum**

The Information Governance Forum has responsibility for overseeing the implementation of the Information Governance Strategy incorporating Framework, and the Information Governance Policy. The Forum is also responsible for the annual Information Management Controls Assurance Standard (IM CAS) assessment and oversees and monitors the implementation of the IM CAS 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 standards which encompasses all statutory, mandatory and best practice requirements regarding information management. The Trust’s performance is mandated by the Information
Management Controls Assurance Standard (IM CAS), is reported annually to the Department of Health, Social Services & Public Safety (DHSSPS) and forms a part of the Trust’s assurance processes.

(Please also refer to the Trust’s Information Governance Strategy incorporating Framework 2014/15 – 2016/17).

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 1998 will ensure that all personal data it holds is controlled and managed in accordance with the principles of the Data Protection Act 1998, 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 Privacy Impact Assessment (PIA). 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 Information Governance Forum 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 OF THIS POLICY**

The implementation of this Policy is evidenced and monitored through the agenda of the Records Management Committee. The Records Management 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);
- 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.
APPENDICES

Appendix A – Information Risk/Roles and Responsibilities
Appendix B – Key Responsibilities of the SIRO
Appendix C – Key Responsibilities of the IAO
Appendices

Appendix A - Information Risk/Roles and Responsibilities

Accountable Officer

Chief Executive

• Receive advice
• Statement of Internal Control
• Receive SIRO Annual Report
• Receive Regular reporting

SIRO

Director of Performance and Reform

• Own Risk Policy/Review
• Own Risk Assessment Process
• Information Risk Action Plan
• Advise on Information Risk Issues
• Receive risk reviews
• Provide regular advice/assurance
• Undertake training.

IAO

IAO

IAO

• Authorise Information Asset Transfers
• Provide/receive regular advice
• Create/maintain own IA register
• Conduct biannual review of owned assets
• Provide annual written Risk Assessment to SIRO via HOS IG
• Authorise requests for access
• Undertake Training
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.