**Information Governance Policy**  
Includes Strategy and Management Framework  
Version: 5

<table>
<thead>
<tr>
<th><strong>Summary:</strong></th>
<th>This policy provides the Information Governance Framework required to ensure compliance with relevant legislation, and for effective management and protection of organisational and personal information.</th>
</tr>
</thead>
</table>
| **Keywords (minimum of 5):**  
*(To assist policy search engine)* | Information; governance; strategy; records; management; data protection; security; confidentiality; quality; regulations; GDPR; DSPT |
| **Target Audience:** | All staff employed by Southern Health NHS Foundation Trust, Non-Executive Directors and Contractors. |
| **Next Review Date:** | March 2020 |
| **Approved and ratified by:** | Information Governance Group  
**Date of meeting:**  
11/03/2019 |
| **Date issued:** | March 2019 |
| **Brief summary of changes:** | Update of legislation and requirements |
| **Author:** | Lesley Barrington, Head of Information Assurance |
| **Accountable Executive Lead:** | Finance Director |
### Version Control

#### Change Record

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Page</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/01/2012</td>
<td>L Barrington</td>
<td>V1.2</td>
<td>All</td>
<td>Minor amendments following IGG group consultation</td>
</tr>
<tr>
<td>25/06/2015</td>
<td>L Barrington</td>
<td>V2</td>
<td>All</td>
<td>3 year review. Updated to include: Update of current IG Framework Update of legislation and regulations</td>
</tr>
<tr>
<td>05/10/2016</td>
<td>L Barrington</td>
<td>V3</td>
<td>All</td>
<td>Update and review. Following recommendation from ICO Audit completed in October 2015 for annual review of IG policy</td>
</tr>
<tr>
<td>16/01/2018</td>
<td>L Barrington</td>
<td>V4</td>
<td>All</td>
<td>Update and review to incorporate new General Data Protection Regulations (GDPR) implementing in May 2018.</td>
</tr>
<tr>
<td>31/01/2019</td>
<td>L Barrington</td>
<td>V5</td>
<td>All</td>
<td>Annual review – minor amendments and updates</td>
</tr>
</tbody>
</table>

### Reviewers/contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Version Reviewed &amp; Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Les Sharpe</td>
<td>Interim Information Governance Manager</td>
<td>V0.1 Aug 2011</td>
</tr>
<tr>
<td>Information Governance Group</td>
<td>Membership &amp; Divisional IG Leads</td>
<td>V1.2 09/01/2012</td>
</tr>
<tr>
<td>Information Governance Group</td>
<td>Membership and Leads:</td>
<td>V2 July 2015</td>
</tr>
<tr>
<td></td>
<td>Lisa Franklin – Director</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Liz Taylor – Assoc. Director Children’s</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rachel Lloyd – Records Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ed Purcell – Info Security Specialist</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sharon France – Info Governance Manager</td>
<td></td>
</tr>
<tr>
<td>Information Governance Group</td>
<td>Membership and Leads</td>
<td>V3 October 2016</td>
</tr>
<tr>
<td>Information Governance Group</td>
<td>Caldicott Guardian</td>
<td>V3 18/10/2016</td>
</tr>
<tr>
<td>Information Governance Group</td>
<td>Membership and Leads</td>
<td>V4 13/03/2018</td>
</tr>
<tr>
<td>Information Governance Group</td>
<td>Membership and Leads</td>
<td>V5 11/03/2019</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Governance Strategy Statement</strong></td>
<td>4</td>
</tr>
<tr>
<td><strong>Information Governance Policy – Management &amp; Framework</strong></td>
<td></td>
</tr>
<tr>
<td>1. Introduction</td>
<td>6</td>
</tr>
<tr>
<td>2. Who does this policy apply to?</td>
<td>6</td>
</tr>
<tr>
<td>3. Definitions</td>
<td>6</td>
</tr>
<tr>
<td>4. Duties/ responsibilities</td>
<td>7</td>
</tr>
<tr>
<td>5. Main policy content</td>
<td>6</td>
</tr>
<tr>
<td>5.2 National Data Security Standards</td>
<td>7</td>
</tr>
<tr>
<td>5.3 Information Governance Group</td>
<td>9</td>
</tr>
<tr>
<td>5.5 Incident Reporting</td>
<td>9</td>
</tr>
<tr>
<td>6. Training requirements</td>
<td>10</td>
</tr>
<tr>
<td>7. Monitoring compliance</td>
<td>10</td>
</tr>
<tr>
<td>8. Policy review</td>
<td>11</td>
</tr>
<tr>
<td>9. Associated documents</td>
<td>11</td>
</tr>
<tr>
<td>10. Supporting references</td>
<td>11</td>
</tr>
</tbody>
</table>

### Appendices

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Training Needs Analysis (TNA)</td>
<td>12</td>
</tr>
<tr>
<td>A2</td>
<td>Equality Impact Assessment (EqIA)</td>
<td>13</td>
</tr>
<tr>
<td>A3</td>
<td>Legal and Regulatory Framework</td>
<td>14</td>
</tr>
<tr>
<td>A4</td>
<td>Information Governance Group – terms of reference</td>
<td>15</td>
</tr>
</tbody>
</table>

SH IG 17 Information Governance Policy
Version 5
March 2019
INFORMATION GOVERNANCE STRATEGY

Strategy statement:

This strategy sets out the approach taken within Southern Health NHS Foundation Trust (the Trust) to provide a robust Information Governance (IG) Management Framework, for the current and future management of information, and compliance with required legislation.

Any associated resource implications incurred by the implementation of the IG Strategy and Policy, will be identified by the IG Group, and reported to the Trust Board as appropriate and required.

This strategy sets out to further develop and implement a change in culture towards IG by all staff. IG is a key component of performance management, i.e. it is central to the working practices of all staff, of all grades and roles, permanent or temporary, working within the Trust.

Through the implementation of the IG Policy, the Trust will:

1. establish robust information governance processes conforming to the law, NHS and Department of Health standards
2. ensure that all policies and procedures relating to the processing of personal information, including handling and holding personal and Trust corporate information are legal and conform to best and/or recommended practice
3. ensure that clear information is given to patients, families and carers, and staff about how their personal information is recorded, handled, stored and (if required) shared by the Trust. The public will be provided with guidance, available in various formats, to explain their rights, how their information is handled, how they can obtain further information and how they can raise concerns. This is published in the Privacy Notice that is included on the public website.
4. provide clear advice and guidance to staff and ensure that they understand and apply the principles of Information Governance to their working practices in relation to protecting the confidentiality and security of personal information and to ensure the safekeeping and handling of Trust business information, and compliance with appropriate legislation
5. ensure that procedures are reviewed on a regular basis to monitor their effectiveness in order that improvements or deficiencies in information handling standards can be recognised and addressed
6. work to embed an Information Governance culture in the Trust through increasing awareness and providing training on the key issues
7. maintain a clear reporting structure and ensure that through management action and training all staff understand the IG requirements
8. undertake regular reviews and audits of how information is recorded, held and used. Audits will be used to identify good practice
9. ensure that there are robust procedures for notifying and learning from IG breaches and incidents in line with the Incident Reporting Policy (SH IG 62)
10. ensure improvement plans are developed and agreed in response to the NHS Digital Data Security and Protection Toolkit, (DSPT) developing and taking forward improvement plans pertaining to the current toolkit, and reporting progress to the Information Governance Group on a regular basis.
11. Ensure that the National Data Security Standards are embedded in the IG culture, including continuing to highlight and manage/mitigate risks to cyber security.
Implementation of these strategic aims and objectives are included in the policy (below) and in associated documents (guidance, standards and procedures), and by the annual submission of the Data Security and Protection Toolkit. This work is monitored, reviewed and signed off by the Information Governance Group (IGG) (see Appendix 4).
1. **Introduction**

1.1 Information is the most important asset available to an organisation and therefore all organisations must have robust arrangements for Information Governance (IG) which are reviewed annually and described in the Data Security and Protection Toolkit (DSPT).

1.2 Information Governance is owned by the Trust’s most senior management and this is demonstrated by signing annually a Statement of Compliance via the DSPT in respect to the Trust and any contracted services.

1.3 IG Compliance is supported by the key roles of Caldicott Guardian, Senior Information Risk Officer (SIRO), Data Protection Officer and Head of Information Assurance, who is supported by the Information Assurance Team. However, all staff have a duty of confidentiality, and an important role to play in ensuring the Trust achieves its strategic objectives.

1.4 IG Compliance is also supported by the identification of Information Asset Owners, Administrators, Information Mapping and Information Asset Registers through a process of risk management.

1.5 Information security is managed through the Information Governance Group and the Information Management and Technology Strategy Forum (IM&T).

2. **Who does this policy apply to?**

2.1 All staff within SHFT, both permanent and temporary, who either use information “owned” by the Trust, or requiring access to information “owned” by the Trust.

3. **Definitions**

3.1 The term **Information Governance** describes the structures, policies and practices used to ensure the confidentiality and security of the clinical records of patients/service users; employment records relating to staff and Trust corporate business.

3.2 **“Information”** includes information in any media - including paper records and electronic data: clinical records, letters, emails, CDs, DVDs, x-rays, patient administration systems/electronic patient record systems; corporate information including staff records; financial records and estates and facilities records.

3.3 This includes the equipment that gathers or stores the above – e.g. computers (networks, desktops), laptops, smart phones, paper records stores.

3.4 **Legal and Regulatory Framework**

There are a number of legal obligations placed upon the Trust for the use and security of personal and confidential information. Refer to Appendix 3 for detail.

The Trust is registered with the Information Commissioners Office as a Data Controller and processor of information, and must comply with its duties as defined by this registration.
Refer to SH IG 18 Data Protection and Confidentiality Policy for detail.

4. Duties / Responsibilities

4.1 Board Responsibility
It is the role of the Trust Board to define the organisation’s policy in respect of Information Governance taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

4.1.1 The Senior Information Risk Officer (SIRO) has ultimate responsibility for the management and mitigation of risks associated with the Trusts information management processes. The SIRO is the chair of the IGG, although this is routinely delegated to the Director of Information & Technology who is the Delegated SIRO.

4.1.2 The Caldicott Guardian is responsible for ensuring that Caldicott principles are followed – refer to the Data Protection & Confidentiality Policy (SH IG 18) for detail.

4.1.3 The Data Protection Officer provides the organisation independent risk-based advice to support its decision-making in the appropriateness of processing Personal and Special Categories of Data within the Principles and Data Subject Rights laid down in the General Data Protection Regulation (GDPR).

4.1.3 The Head of Information Assurance has particular responsibility for providing guidance on all areas of Information Governance, ensuring relevant legislation and guidance are incorporated into Trust practice via the Information Governance Group and providing leadership and management of the Information Assurance Team.

4.2 Managerial Accountability and Responsibility
All line managers from all operational and corporate services within the Trust are responsible for ensuring that the policy and its supporting strategy, standards, procedures and guidelines are built into local processes and there is ongoing compliance. Breaches of policy will be handled in line with the Trusts Disciplinary Policy (SH HR 28).

4.3 Individual Responsibility
Every individual staff member (both permanent and temporary) and contractors are responsible for ensuring they are aware of the requirements incumbent upon them and for ensuring they comply with these on a day to day basis. Any staff member who does not comply with this policy, or breaches the confidentiality of patients/staff, will be subject to Disciplinary Procedures as per Trust policy, which may result in their dismissal, and if professionally registered, reported to their professional body.

5. Main policy content

5.1 The aim of the policy and management framework is to ensure compliance with the strategic objectives and legal obligations above and DSPT requirements. A schedule of DSPT compliance is an integral part of the IG work plan which is regularly reviewed and updated at the Information Governance Group (IGG).

5.2 National Data Security Standards
The agenda of the IGG is structured around the National Data Guardian’s 10 Data Security Standards:
### Leadership Obligation 1

**People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles**

<table>
<thead>
<tr>
<th>Data Security Standard 1</th>
<th>All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security Standard 2</td>
<td>All staff understand their responsibilities under the National Data Guardian’s Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.</td>
</tr>
<tr>
<td>Data Security Standard 3</td>
<td>All staff complete appropriate annual data security training and pass a mandatory test, provided through the redesigned Data Security and Protection Toolkit (or provide similar via in-house training programmes).</td>
</tr>
</tbody>
</table>

### Leadership Obligation 2

**Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses**

<table>
<thead>
<tr>
<th>Data Security Standard 4</th>
<th>Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security Standard 5</td>
<td>Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.</td>
</tr>
<tr>
<td>Data Security Standard 6</td>
<td>Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.</td>
</tr>
<tr>
<td>Data Security Standard 7</td>
<td>A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.</td>
</tr>
</tbody>
</table>

### Leadership Obligation 3

**Technology: Ensure technology is secure and up-to-date.**

<table>
<thead>
<tr>
<th>Data Security Standard 8</th>
<th>No unsupported operating systems, software or internet browsers are used within the IT estate.</th>
</tr>
</thead>
</table>
| Data Security Standard 9 | A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such
5.3 Information Governance Group

The Information Governance Group (IGG) is accountable to the Trust Audit, Assurance & Risk Committee, via the IM&T Forum, and holds overall responsibility to ensure the Trust adheres to the Information Governance Policy.

The Terms of Reference for the IGG can be found in Appendix 4, which includes the full membership, reporting structure and administrative arrangements.

The IGG agenda is structure to monitor compliance with the National Data Security Standards (above) and sign off completion of the NHS Digital Data Security & Protection Toolkit.

5.4 Other objectives/purposes of the IGG include:

- ensuring that all IG policies, procedures and guidance are published on the Trust website, disseminated via the IG Leads, and regular updates and learning from incidents are published via an Information Assurance Newsletter. Policies are reviewed at least 3 yearly, or sooner if there are changes to legal or regulatory obligations
- ensuring that the Information Asset Management Framework is maintained and up-to-date
- receiving reports on Data Quality and secondary processing
- ensuring compliance with the Public Records Act 1958 with regard to the management of Corporate Records; receiving reports from the Corporate Records Group with regard to the implementation of the work plan, and compliance with the NHS Code of Practice: Records Management 2016
- receiving reports with regard to Freedom of Information Act 2000
- receiving reports with regard to Subject Access Requests under the Data Protection Act/GDPR

5.5 Incident reporting:

5.5.1 Failure to comply with this policy may result in breaching the GDPR/Data Protection Act (and other legal and regulatory) requirements, resulting in a fine from the Information Commissioner. Where there is a breach of confidentiality or loss of data or information asset, this must be reported and managed via the incident reporting process (via the incident reporting system Ulysses), and SH IG 62 Information Governance Incident Reporting Procedure.

5.5.2 All serious incidents, known as IG SIs, must be rated using the risk assessment contained in SH IG 62. If the outcome of the risk assessment and investigation identifies the incident as a score of 6 or above, the incident, must be recorded and reported via the NHS Digital Incident Reporting Tool on the NHS Digital DSPT. This will automatically result in a referral to the Information Commissioner’s Office. Any potential serious IG incident must be reported to the Information Assurance Team as soon as possible, who will support the service to conduct an Initial Management Assessment (IMA). Once this is completed, and the incident is confirmed as a Serious IG Incident, with a risk factor of 6 (or above), the Information Assurance Team will then inform the Head of Information Assurance, Director of Information &
Technology, SIRO, Data Protection Officer and Caldicott Guardian that a report is to be made.

The Information Assurance Team will update the NHS Digital DSPT reporting tool on a regular basis with regard to the management of the incident, and any response received from the Information Commissioners Office regarding the outcome. Once all actions have been taken to manage the incident, mitigate any risks, and implement the agreed action plan, the incident will be closed.

5.5.3 The Information Governance Group will receive regular reports of incidents; analysis of trends and review copies of Incident Management Reports to ensure the mitigation of the risk, and share learning across the Trust.

6. Training Requirements

6.1 Permanent new staff will receive information governance training as part of their Induction via an on-line eLearning package with eAssessment. Face to face bespoke training is also available on request from the Information Assurance Team to meet learning needs.

6.2 Annual mandatory on-line e-learning Information Governance training is required for all employed staff (both permanent and temporary). This is available from the LEaD training tool and links directly to an individual’s training record. Facilitated face to face sessions are available on request from the Information Assurance Team for staff who do not have access to a computer or require additional training support.

6.3 In addition some roles are required to complete additional annual training, (e.g. the Data Protection Officer; SIRO, Caldicott Guardian, IT Security Specialist) which is available via the NHS Digital e-learning site: https://nhsdigital.elfh.org.uk/login

6.4 Compliance with the mandatory annual training is included in all services Performance Review Dashboards, and monitored at Division Performance Reviews and at the IGG.

See Appendix 1 – Training TNA.

7. Monitoring compliance

7.1 As a Foundation Trust, and as stipulated in the Operating Framework, the Trust is required to be compliant with the DSPT. Failure to maintain this would mean that the Trust would be unable to tender for new business.

7.2 Additionally, the Information Commissioners Office monitors all serious breaches of personal information and/or confidentiality, and could impose a statement of undertaking, or ultimately a financial penalty.

7.3 The Information Governance Group (IGG) is responsible for ensuring an assessment of compliance as detailed in the DSPT is undertaken each year. Annual work / development plans are produced and these are considered by the IGG at the bi-monthly meetings throughout the year and reviewed before the required annual submission.

Reports on progress are provided to the SIRO, Data Protection Officer and Caldicott Guardian, via the IM&T Strategy Board and Audit, Assurance and Risk Committee as required.
8. **Policy Review**

8.1 This policy will be subject to review on an annual basis (or sooner if new legislation, codes of practice of national standards are introduced).

9. **Associated Documents**

   SH IG 18 Data Protection and Confidentiality Policy  
   SH IG 12 Access to Personal Records Procedure  
   SH IG 13 Information Life Cycle Policy  
   SH IG 46 Information Sharing Policy  
   SH IG 61 Overarching Information Security Policy  
   SH IG 53 ICT Security Policy and associated procedures  
   SH IG 43 Registration Authority Policy  
   SH NCP 2 Data Quality Policy

10. **Supporting References**

   - Data Security & Protection Toolkit: [https://www.dsptoolkit.nhs.uk/](https://www.dsptoolkit.nhs.uk/)  
     - RW1 SHFT organisation code  
   - Information Commissioners Office: [https://ico.org.uk/](https://ico.org.uk/)  
     - Data Protection Act  
     - Freedom of Information Act  
     - Records Management Code of Practice  
### Appendix 1: Training Needs Analysis

<table>
<thead>
<tr>
<th>Training Programme</th>
<th>Frequency</th>
<th>Course Length</th>
<th>Delivery Method</th>
<th>Facilitators</th>
<th>Recording Attendance</th>
<th>Strategic &amp; Operational Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Governance – Introduction and Annual Re-fresher</td>
<td>Annually</td>
<td>Approx. 1 hour</td>
<td>eLearning or eAssessment via LEAD training tool</td>
<td>Information Assurance Team</td>
<td>Individual log-into system</td>
<td>Director of Information &amp; Technology Head of Information Assurance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Directorate</th>
<th>Service</th>
<th>Target Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMH/LD/OPMH</td>
<td>Adult Mental Health</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specialised Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Learning Disabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Older Persons Mental Health</td>
<td></td>
</tr>
<tr>
<td>ISD’s</td>
<td>Adults</td>
<td>All staff</td>
</tr>
<tr>
<td>ISD’s</td>
<td>Children’s Services</td>
<td></td>
</tr>
<tr>
<td>Corporate</td>
<td>All</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 2: Equality Impact Assessment

The Equality Analysis is a written record that demonstrates that you have shown due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations with respect to the characteristics protected by the Equality Act 2010.

Stage 1: Screening

<table>
<thead>
<tr>
<th>Date of assessment:</th>
<th>31/01/2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of person completing the assessment:</td>
<td>Lesley Barrington</td>
</tr>
<tr>
<td>Job title:</td>
<td>Head of Information Assurance</td>
</tr>
<tr>
<td>Responsible department:</td>
<td>Technology</td>
</tr>
<tr>
<td>Intended equality outcomes:</td>
<td></td>
</tr>
</tbody>
</table>

Who was involved in the consultation of this document? Information Governance Group

Please describe the positive and any potential negative impact of the policy on service users or staff.

In the case of negative impact, please indicate any measures planned to mitigate against this by completing stage 2. Supporting Information can be found be following the link: www.legislation.gov.uk/ukpga/2010/15/contents

<table>
<thead>
<tr>
<th>Protected Characteristic</th>
<th>Positive impact</th>
<th>Negative impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>This policy ensures that all information created, maintained and disposed of by the Trust complies with legislation and national NHS requirements</td>
<td></td>
</tr>
<tr>
<td>Disability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender reassignment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marriage &amp; civil partnership</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pregnancy &amp; maternity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Religion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sexual orientation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Stage 2: Full impact assessment

<table>
<thead>
<tr>
<th>What is the impact?</th>
<th>Mitigating actions</th>
<th>Monitoring of actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix 3

Legal and Regulatory Framework:

The Trust is bound by the provisions of a number of laws and regulations. The list below is not exhaustive, and other legislation and regulations may also apply.

Laws:

- UK Data Protection Act 2018
- General Data Protection Regulations
- Health & Social Care (Quality & Safety) Act 2015
- Common Law Duty of Confidentiality
- Health & Social Care Act 2012
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Crime and Disorder Act 1998
- Road Traffic Act 1988
- Electronic Communications Act 2000
- Public Interest Disclosure Act 1998

Regulations:

- Caldicott Committee Report 2013
- NHS Confidentiality Code of Practice 2003
- DoH Records Management: Code of Practice 2016
- Care Quality Commission Standards
1. Introduction

Information Governance provides a framework to bring together the requirements, standards and best practices that apply to the handling of information; ensuring information is accurate, dealt with legally, securely and efficiently in order to deliver the best possible care.

The principles of Information Governance (IG) include:
- Compliance with Data Protection law (inc. General Data Protection Regulation – GDPR)
- Information Governance Policies and Procedures – including compliance with the 10 National Data Security Standards
- Data Security and Cyber Management
- Confidentiality and Caldicott Guidance
- Data Quality
- Secondary Use
- Corporate Information Management

2. Purpose

The purpose of the Information Governance Group (IGG) is to:
- provide a forum for the discussion, acknowledgement and sign off of the IG Management Framework
- Review and sign off policies and procedures as required by the IG Management Framework
- Review Caldicott/confidentiality issues, including access to electronic systems; review of incidents relating to breaches of confidentiality and other issues as required.
- Ensure compliance with NHS Digital Data Security & Protection Toolkit (DSPT) assurances, including mandatory training compliance
- Share knowledge and learning from IG incidents, and issues raised by the Information Commissioner’s Office

The group will provide advice and assurance to the Trust on all matters concerning Information Governance and will coordinate, supervise and direct the work necessary to provide a co-ordinated corporate approach to Information Governance.

Accountable to the Trust Board via the Data Protection Officer, SIRO and Caldicott Guardian, bi-monthly updates will be made to the Information Management & Strategy Forum to coincide with the national DS&PT submissions; and IG contribution to Trust Board.


3. Objectives

The objectives of IGG include:

3.1 the provision of a Trust wide effective suite of Information Governance Policies, procedures, guidance and management arrangements which are regularly reviewed in line with changes in legislation and regulatory requirements, including:
• Maintaining a balance between openness and confidentiality
• Legal compliance (e.g. Data Protection, Freedom of Information and other relevant legislation)
• Information security (including cyber security, confidentiality, information sharing, integrity and availability)
• Information quality assurance
• Records management

3.2 ensuring compliance with the DS&PT, ensuring all 10 Data Security Standards are met and evidence is uploaded into the NHS Digital on-line tool

3.3 to comply with Care Quality Commission Standards, NHSLA Standards, Department of Health Codes of Practice, Clinical Negligence Scheme for Trusts, the ISN for Information Governance

3.4 ensuring compliance with the recommendations and commitments identified in the Caldicott 2 Review

3.5 providing support and structure to the Data Protection Officer; Senior Information Risk Owner (SIRO), the Caldicott Guardian and the Head of Information Assurance and Information Assurance Team.

3.6 developing and maintaining an IG Development Plan to address all Information Governance improvements, including securing necessary resources and monitoring the implementation of the plan

3.7 providing reports to the Information Management and Strategy Forum via the Delegated SIRO (chair) regarding compliance with the DSPT annual submission (usually end of March)

3.8 Receiving and approving Data Privacy Impact Assessments and Information/Data Sharing Agreements

3.9 receiving and considering reports into breaches of IG/confidentiality and where appropriate undertake or recommend remedial action; including sharing the learning, and reporting on concerns raised by the Information Commissioner’s Office

3.10 via the Information Asset Register, ensuring IG risks are identified, assessed, mitigated and regularly reviewed and when appropriate recorded on the Trust Risk Registers

3.11 receiving requests and maintain a register of Access Requests and Approvals to SHFT Electronic Patient Records Systems (e.g. OpenRiO)

3.12 promoting Information Governance throughout the Trust Clinical and Corporate divisions via IG Leads, ensuring that all staff receives annual IG training

Membership

Membership of IGG will include
• Data Protection Officer (joint Chair)
• Senior Information Risk Officer (SIRO)
• Director of Information & Technology (joint Chair)
• Caldicott Guardian
• Associate Director of Technology
• Head of Information Assurance
• Information Governance Manager
• Information Security Specialist
• Head of Information
• Quality & Governance Manager (FOI Lead)
• Head of Estates and Facilities Management
• Head of Finance
• Senior HR Manager – Workforce Information & Systems
• Chief Clinical Information Officer (CCIO)
• Divisional/Service Information Governance Leads (MH LD HR, Finance, Integrated Service Divisions, Children’s Services. See Appendix one for role of IG Lead)
• Learning, Education and Development Representative

-o And others by invitation
-o Deputies to attend as necessary to ensure all divisions are represented

**Quorum** is constituted when the Data Protection Officer, Caldicott Guardian, SIRO, Delegated SIRO or Head of Information Assurance is present and at least 4 members.

**Frequency of Meetings**

Meetings will be bi-monthly or as required. The use of teleconferencing for sign off to be used as required.

IGG TOR v.1 for signed off 10/10/2011
Review date: March 2012
IGG TOR v.2 signed off 09/07/2012
Review date: July 2013
IGG TOR v.3 13/05/2013
Review date: 08/07/2013
IGG TOR v.4 14/07/2014
Review date July 2015
IGG TOR v.5 13/07/2015  IGG TOR v.5.1 11/01/2016 (ICO Audit recommendations)
Review date July 2016
IGG TOR v.6 04/10/2016 Draft Virtual Sign Off.
IGG TOR v7 11 09 2017 Sign Off 11/9/2017
Review date March 2018
IGG TOR v8 29/05/2018 Sign off 09/07/2018

**Annex 1 – Role of Data Protection Officer (joint chair)**

Key responsibilities:

- To Chair and Lead the IGG
- To ensure the IG Development Plan and delivery is in line with legal and national requirements
- To inform and advise the organisation (Executive and Trust Board) and its employees about their obligations to comply with the GDPR and other data protection laws
- Via the IGG - to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits