

Information Governance Policy and Strategic Management Framework

Including the Information Governance Strategy

|  |  |
| --- | --- |
| **Directorate Responsible for Policy:** | Chief Executive |
| **Name of responsible board/committee:** | IGSG |
| **Post Holder Responsible for Policy:** | IA/RA, Data Protection Manager |
| **Contact Details:** | Heidi.doubtfire@nhs.net |
| **Date Written:** | October 2018 |
| **Approved By:** | IGSG |
| **Date Approved:** | 01/10/2018 |
| **Ratified by:** | OMB |
| **Date ratified:** | 16/10/2018 |
| **Date Policy Becomes Live:** | 16/10/2018 |
| **Reviewed:** | 18/02/2020 |
| **Next Due for Review:** | 17/02/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version No.** | **Updated By** | **Updated On** | **Description of Changes** |
| 1.0 | IG/RA Manager & DPO | 11/10/2018 | Final version for OMB |
| 1.1 | IG Officer | 25/03/2019 | Updated emails (NHS Migration) |
| 1.2 | IG/RA Manager & DPO | 25/11/2019  Approved 18/02/2020 | New Governance Structure  Role of SIRO Change  New role of Chief Information Officer |
| 1.3 | IG/RA Manager & DPO & IG Officer | 07/10/2020 | Sent to the Corporate Records Committee for comments for meeting 29.07.2020. Comment deadline extended to 07.08.2020. Changes made: Updated Trust’s Management Structures. Expanded the Records Management in Section 13 with DIRKS information. Added CRMC Guardian overview to appendices. Links created to the Employee & Managers Handbooks 07.10.2020 Section 5.1 was expanded by the Information Services Manager - the Data Quality Procedure and Records Management Procedure now support quality assurance and the effective management of records. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Section A – IG Policy 6](#_Toc27577774)

[1. Policy Statement, Aims & Objectives 6](#_Toc27577775)

[Table 1: KPIs and method of assessment 7](#_Toc27577776)

[2. Legislation and Guidance 7](#_Toc27577777)

[3. Scope 8](#_Toc27577778)

[4. Responsibilities and Accountability 8](#_Toc27577779)

[Table 2: Responsibility is also delegated to the following individuals. 8](#_Toc27577780)

[5. Training 14](#_Toc27577781)

[Section B – IG Policy and Strategic Management Framework 15](#_Toc27577782)

[1. Introduction 15](#_Toc27577783)

[Diagram 1: Overall reporting structure 17](#_Toc27577784)

[Diagram 2: Information Governance reporting structure 18](#_Toc27577785)

[2. Strategic Aims 19](#_Toc27577786)

[Table 3: Strategic Aims 19](#_Toc27577787)

[3. Openness, Transparency and Information Sharing 27](#_Toc27577788)

[4. Information Security 28](#_Toc27577789)

[5. Information Quality Assurance/Data Quality 29](#_Toc27577790)

[6. Data Protection 29](#_Toc27577791)

[Table 4: Six Data Protection Principles 30](#_Toc27577792)

[Table 5: GDPR principles and expectations 31](#_Toc27577793)

[Diagram 3 - Data Protection Officer/IG Manager’s Accountability Framework 32](#_Toc27577794)

[7. Confidentiality 33](#_Toc27577795)

[Diagram 4 - Caldicott Guardian Accountability and Organisational Framework 34](#_Toc27577796)

[Table 6: Caldicott Principles 34](#_Toc27577797)

[8. Information Risk Management Framework 35](#_Toc27577798)

[Diagram 5 - Senior Information Risk Owner Accountability Framework 36](#_Toc27577799)

[Diagram 6 - Chief Information Officer – DPST assurance / escalation / sign off process 36](#_Toc27577800)

[9. Information Asset Management 38](#_Toc27577801)

[Table 7: The six main categories of information asset: 38](#_Toc27577802)

[Diagram 7 - internal information risk management reporting accountability framework 39](#_Toc27577803)

[Diagram 8 – Communications SIRO, IAO, IAA 41](#_Toc27577804)

[10. Data Management 42](#_Toc27577805)

[11. Information Technology (IT) Asset Management 42](#_Toc27577806)

[12. Freedom of Information and Environmental Information Regulations 2000 43](#_Toc27577807)

[13. Records Management / Information Lifecycle Management 44](#_Toc27577808)

[14. Improvement Plan and Assessment 46](#_Toc27577809)

[15. Employee and Managers’ Handbooks: Your Roles and Responsibilities for IG 46](#_Toc27577810)

[Section C – IG Standard Operating Procedures 48](#_Toc27577811)

[Diagram 9 - Internal and External Information Governance, Data Protection, Confidentiality, and Security Assurance Framework 48](#_Toc27577812)

[Appendices 49](#_Toc27577813)

[Appendix C: IG Training Needs Analysis for 2018-2020 50](#_Toc27577814)

[Appendix D - IG Standard Operating Procedure Structure 52](#_Toc27577815)

[Appendix E - Offences relating to personal data 54](#_Toc27577816)

[Appendix F - External Governance, oversight, enforcement and reporting arrangements within the NHS 58](#_Toc27577817)

[Appendix G - Corporate Records Management Committee Guardians 63](#_Toc27577816)

**DEFINITIONS**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Access Control | Restrictions to accessing information |
| Accountability | Responsibility for all aspects of data security |
| Anonymised information | Data that has had all personal identifiable data removed |
| Caldicott Guardian | Person responsible for ensuring that all data protection, and NHS obligations are fulfilled |
| Confidentially | Keeping data secure |
| Consent | Specific permission from the data subject |
| Data controller | Organisation that owns the data |
| Data minimisation | The least amount of information need to process the data |
| Data processor | Organisation that works with the data on behalf of the Controller |
| GDPR | EU General Data Protection Regulation |
| IAA | Information Asset Administrator – person who manages the status of data |
| IAO | Information Asset Owner – person responsible for the data |
| Information Governance | How data is correctly managed within the NHS |
| Information Lifecycle Management | Managing the flow of an information system's data from creation and initial storage to the time when it becomes obsolete and is deleted |
| Information Risk | Opportunities for data to be accessed by unauthorised people |
| Password | Specific code to access information |
| Personal confidential data | Individual’s information |
| Processing of data | Storing, using, recording, and deleting data |
| Pseudonymised data | Shared data that has the personal identifiable information removed and replaced with a code so that the controller can identify the individual. |
| Risk assessment | Check of processes to identify where errors may occur |
| Risk management | How identified risks will be reduced, mitigated, or accepted. |
| Safe Haven | An agreed set of arrangements that are in place to ensure confidential person identifiable information can be communicated safely and securely |
| Security breach | Unauthorised access to data |
| SIRO | Senior Information Risk Owner |
| Sensitive/special categories of personal data | Information beyond personal identification, e.g. sexual orientation, religious beliefs, etc. |

# Section A – IG Policy

## Policy Statement, Aims & Objectives

Salisbury NHS Foundation Trust fully supports the principles of information governance, recognising its public accountability, but equally placing importance on the confidentiality of, and the security arrangements to safeguard personal information about patients, employees and commercially sensitive information, and for implementing risk management and embedding risk management into the culture of the organisation.

* 1. This document sets out the Trust’s policy for Information Governance within the organisation. This policy includes the Information Governance Framework and all associated procedures.
  2. The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Equal importance is placed on the confidentiality of, and the security arrangements to safeguard personal information about patients and employees, and commercially sensitive information. The organisation also recognises the need to safely share patient information with other health organisations and other partner care organisations, with the explicit consent of the patient or where there is a legal gateway to share. In certain circumstances information may be shared with other agencies in the public interest in line with agreed protocols.
  3. Information Governance plays a key part in supporting clinical and corporate governance. The organisation recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. It also gives assurance to the organisations and to individuals that personal information is dealt with legally, securely, efficiently and effectively.
  4. There are 6 principal areas which form the scope of Information Governance:
* Information Governance Management
* Confidentiality and Data Assurance
* Information Security Assurance
* Clinical Information Assurance
* Data Quality Assurance
* Corporate Information Assurance
  1. The aims of this document are to:
* Provide employees with a framework through which all the elements of Information Governance and Data Protection will be met;
* Ensure a proactive use of information within the organisation both for patient care and service management as determined by law, statute and best practice;

and ensures that:

* the Trust complies with the requirements contained in the Data Security and Protection Toolkit.
* Information Governance and Data Protection Training is completed by all employees and agency workers on an annual basis.
* robust management and accountability arrangements for Information Governance are in place within the Trust.
* a proactive use of information between the organisation and other NHS and partner organisations to support patient care as determined by law, statute and best practice.
* non-confidential information is made widely available in line with responsibilities under the Freedom of Information Act (2000) and Environmental Information Regulations (2004).
* there are effective arrangements to support confidentiality, security and the integrity of personal and other sensitive information.
* the organisation’s information is of the highest quality in terms of accuracy, timeliness and relevance.
  1. To ensure continuous improvement in information governance the organisation has a range of key performance indicators (KPIs) which it uses for monitoring purposes:

### Table 1: KPIs and method of assessment

|  |  |  |
| --- | --- | --- |
| **No** | **Key Performance Indicators** | **Method of Assessment** |
| **1** | Mandatory compliance of all assertions within the data Security and Protection Toolkit are achieved | Self-assessment completed as required by NHS Digital and annual audit |
| **2** | Mandatory Information Governance training completed by all staff. | Reports through the Operational Management Board (OMB) on Information Governance/Security Training Policy Compliance Reports. |
| **3** | Production of quarterly Standard Assurance reports to the Information Governance Steering Group (IGSG) | Clinical Governance Committee via minutes and exception reports. |
| **4** | Results of the Data Security and Protection Toolkit Compliance | Compliance/Progress Reports |
| **5** | Information Asset Auditing | Compliance/Progress Reports and Risks |
| **6** | Care CERT Compliance | Compliance/Progress Reports and Risks |
| **7** | Policy Compliance | Policy Compliance Reports |

## Legislation and Guidance

The following legislation and guidance has been taken into consideration in the development of this framework:

* Caldicott Guidance (2010)
* Common Law Duty of Confidentiality
* Computer Misuse Act 1990
* Confidentiality NHS Code of Practice (2003)
* Copyrights, Designs & Patents Act 1990
* Crime and Disorder Act (1998)
* Criminal Procedures and Investigations Act (1996)
* Data Protection Act 2018
* Ensuring Security & Confidentiality in NHS Organisations (E5498)
* EU General Data Protection Regulation 2016
* **The Accessible Information Standard 2016 (DCB1605 Accessible Information)**
* EU Network and Information Security Regulations 2018
* Fraud Act 2006
* Freedom of Information Act 2000 & Environmental Information Regulation
* Health and Social Care (Safety and Quality) Act 2015
* Health and Social Care Act (2012)
* HSC 2000/09 Protection & Use of Patient Information
* ICO Framework Codes of Practice
* Information Governance Assurance
* Information Sharing Guidance for Practitioners and Managers
* Information: To Share or Not to Share: Caldicott Reports 2 and 3:Government Response to Caldicott Review (2013)
* NHS Act (2006) and as updated 2012
* Public Interest Disclosure Act 1998
* Public Records Acts 1958 and 1967
* Records Management Code of Practice for Health and Social Care 2016
* Regulatory and Investigatory Powers Act (2000)
* The National Data Guardian for Health and Social Care consultation on the roles and functions 2015
* Privacy and Electronic Communications Regulations (PECR)
* Electronic Identification and Trust Services Regulations (eIDAS)

## Scope

The framework covers all staff, contractors, third party care providers who require access to and the recording of patient data and systems, volunteers and students that create, store, share and dispose of information. It sets out the procedures for sharing information with stakeholders, partners and suppliers. It concerns the management of all paper and electronic information and its associated system repositories regardless of location that affects its regulatory and legal obligations.

## Responsibilities and Accountability

* 1. Overall accountability for ensuring that there are systems and processes to effectively manage information governance lies with the CEO.

It is the responsibility of Executive Directors, Division Clinical Managers, Senior Clinicians, Heads of Departments, Directorate Senior Nurses, Matrons and Ward Sisters/Charge nurses to ensure the implementation of policies throughout their areas of responsibility. Managers must also react in an appropriate manner when informed of instances where behaviour is not in accordance with this framework set out herein.

### Table 2: Responsibility is also delegated to the following individuals.

|  |  |  |
| --- | --- | --- |
| **Position** | **Responsibility** | **Accountability** |
| **Medical Director** | **Caldicott Guardian** | Has delegated responsibility for:   * Acting as the Caldicott Guardian for the organisation with responsibility for clinical information assurance and clinical governance.   **Section 7.3 defines in detail** the Caldicott Guardian Accountability and Organisational Accountability Framework. |

|  |  |  |
| --- | --- | --- |
| **Director of Transformation** | **Senior Information Risk Owner** | Has delegated responsibility for:   * Overseeing the development and maintenance of relevant information governance policies and procedures. Via the Information Governance Steering Group. * Acting as the organisational Senior Information Risk Owner (SIRO), ensuring the identification and mitigation of corporate and operational risks relating to all aspects of information security management. * Ensuring that the organisation meets the requirements of the Information Governance Standards under the Data Security and Protection Toolkit and associated assurance frameworks to ensure that a high level of compliance is reached and maintained by the organisation. * Oversight of the impact of organisational changes on information assets. Ensuring a privacy impact assessment procedure is in place.   **Please refer to section 8.1** whichdefines in detail the SIRO’s Accountability and Organisational Accountability Framework. |
| **IG Manager** | **Data Protection Officer/Privacy Officer** | Has delegated responsibility for:   * Overseeing, coordinating and issuing information governance information, maintaining appropriate records regarding information governance, and monitoring developments in information governance. Ensuring maintenance of the information asset register, information flows, systems and liaising with all teams to ensure this is regularly updated. * Supporting the SIRO in information security management and the Caldicott Guardian on confidentiality and information sharing processes and procedures. * Providing information for patients and staff in relation to how their information is held, used and shared, and answering queries in relation to this, including establishing processes for managing objections. * Operationally managing the organisation’s approach to the creation, storage, sharing, management and disposal of both corporate and clinical records, ensuring compliance with relevant legislation and guidance. * Managing FOIA requests made to the Trust. * Overseeing Information Governance training compliance. * Contributing to governance-related audits and working with Internal Audit to assess progress, developing action plans as required. * Administering information governance related incidents, ensuring the development of action plans and external reporting where appropriate. * Liaising with other committees and groups within the organisation to promote and integrate information governance. * Vice Chairs the Corporate Records Management Committee.   As the named Data Protection Officer has responsibilities under GDPR to:   * provide advice to the organisation and its employees on compliance obligations * advise on when data protection impact assessments are required and to monitor their performance * monitor compliance with the GDPR and organisational policies, including staff awareness and provisions for training * co-operate with, and be the first point of contact for the Information Commissioner * be the first point of contact within the organisation(s) for all data protection matters * be available to be contacted directly by data subjects – the contact details of the data protection officer will be published in the organisation’s privacy notice * take into account information risk when performing the above.   **Please refer to** **section 6.4** which defines in detail the DPO’s Accountability and Organisational Accountability Framework. |
| **Divisional Managers** | **Information Asset Owners** | Information Asset Owners are responsible for providing regular reports to the Senior Information Risk Owner (SIRO) via the IG Department, a minimum of annually on the assurance and usage of their assets. The Information Asset Owners have delegated responsibility for:   * Maintaining professional standards according to best practice in liaison with staff working in the area. * Ensuring local application of guidelines including retention and disposal schedules and advising on disposal. * Determining the most effective ways of promoting the guidelines in their area e.g. training, induction, team meetings etc. * Providing support and advice to staff in the area of Records Management with the assistance of the Caldicott Guardian and Corporate Services. * Monitoring performance through quality control/periodic audits. * Ensuring compliance with the standards, legislation, policies and procedures relating to the management of records. * Identifying areas where improvements could be made. * Ensuring that staff complete relevant training on records management, security, confidentiality, and data protection. * Complying with this policy and procedure in addition to the Manager’s IG Handbook: My roles and Responsibilities for IG. * To effectively manage and efficient Corporate Records within their areas in paper and electronic format. To ensure the Trust complies with its statutory and regulatory obligations.   **Please refer to section 9.2** for details the role of IAOreporting structurewithin the Trust. |
| **Staff** | **Information Asset Administrators** | Information Asset Administrators (IAAs) are employees identified by the Information Asset Owners as being responsible for one or more systems, repositories or applications.   * **Implement** the organisation’s policies * **Understand and address risks** to information assets, and provides assurance to the IAO * **Ensure** compliancewith the organisation’s Information Risk & Security Policy within their area or department * **Co-ordinate** and contribute to risk assessments and mitigation implementation * **Provide** information and reports to the IAO tomaintain relevant parts of the Directorate System Asset Register * **Maintain** an accurate and up to date record of all users for the information asset for which they are responsible, including a record of all user access levels and the timely reporting of discrepancies to the IAO * **Ensure** that the Trust’s requirements for information incident identification, reporting, management and response are followed. This includes the mechanisms to identify and minimise the severity of an incident and the points at which assistance or escalation may be required.   **Please refer to section 9.3** for details the role of IAAreporting structurewithin the Trust |
| **All staff** | **Information Governance** | Responsibilities of Staff (including all employees, whether full/part time, agency, bank or volunteers) are:   * Complying with this framework and associated procedures in addition to the Staff and Manager’s Handbooks: My roles and Responsibilities for IG **Appendix A & B.**   Identifying any gaps in the policy to the responsible officers. |

* 1. The Information Governance Steering Group (IGSG)has delegated responsibility for overseeing information governance management to the Information Governance Group. The IGSG will monitor compliance with Information Governance requirements through standing reports and management activities:
     1. **Compliance Reports:**
* Availability of Patient Records
* Care CERT Compliance Report
* Complaints Report
* Data Protection Impact Assessments Report
* Freedom of Information
* IG/Security Risk Report
* IG/Security Training Report
* Incident Reporting
* Real Time Feedback Report
* Registration Authority Smartcard Compliance
* Subject Access Request
  + 1. **Annual Audit:**
* Clinical Records Audit
* Confidentiality and Protection Audit
* Cyber Essentials Audit
* Data Security and Protection Audit
* Informatics Penetration Audit
  + 1. **Management Activities**

The IGSG will ensure the following management activities are conducted on an annual basis:

* Review the systems in place to develop and implement the Information Governance Policy and all other related procedures.
* Review information incident reporting procedures, monitoring and assuring systems to investigate all reported instances of actual or potential breaches of confidentiality and security.
* Review Information Governance requirements in line with changes on at least an annual basis in order to update contracts, policy and training accordingly.
* Review systems in line with national directives.
* Work with Internal Audit to facilitate effective audits against nationally and locally agreed criteria.
* Support the provision of high quality care by promoting the effective and appropriate use of information.
* Assure the Trust Board that Information Governance policies and procedures remain up-to-date, reflect national guidance and are in operational use throughout the organisation.
* Receive assurance that relevant information governance experience, evidence, research, information and data is readily available to all staff.
  + 1. **Review**

This documentwill be reviewed every three years, and in accordance with the following on an ‘as and when required’ basis:

* Case Law
* Changes in practice
* Changes to organisational infrastructure
* Good practice guidelines
* Legislatives changes
* New vulnerabilities identified
* Significant incidents reported

The IGSG will also ensure that this Information Governance Policy and Strategic Management Framework are used in conjunction with the policy and will act as an overarching framework for the local delivery of Information Governance.

* + 1. **Monitoring**

This policy will be performance monitored to ensure that it is in-date and relevant to the core business of the Trust. The results will be published in the regular policy compliance report submitted to the Operational Management Board (OMB)

* 1. **The Information Governance Steering Group’s (IGSG) purpose is to:**
* Guide the Trust as a data controller, in ensuring that all information is used in line with legislation/standards using members’ roles and expertise to direct work plans;
* Directly support the Senior Information Risk Officer, Caldicott Guardian and Data Protection Officer roles;
* Maintain the Trust's notification with the Information Commissioner’s Office;
* Ensure objections to the disclosure of confidential personal information are appropriately respected (where applicable);
* Ensure completion of the DPST and General Data Protection Regulations (GDPR) and equivalent each year;
* Approve any action plans stemming from the IG work plan and monitor their implication;
* Review and maintain all related policies / procedures on behalf of the Trust;
* Review any risks or incidents in relation to Information Governance and ensure that appropriate actions have been taken and an escalation process is implemented and monitored for IG incidents;
* Ensure that the Trust's approach to information handling is communicated to all staff and made available to the public (where applicable) by reviewing training programmes, fair processing notices and communication plans;
* Review the results of any Information Governance audits and oversee the implementation of any remedial actions;
* Review minutes and actions of meetings with the SIRO and Caldicott Guardian;
* Review the presentation of the Data Security and Protection Toolkit (DPST) progress, reports, incidents, and risks regarding IG requirements and ensure that assurance is received for actions being implemented;
* Conduct key reviews of the Information Asset Register with Information Asset Owners linking Data Protection Impact Assessments (DPIA);
* The Information Governance Steering Group shall take place on a quarterly basis with a key membership including the Director of Transformation (SIRO), Caldicott Guardian, DPO, Chief Information Officer, Head of IT, as well as the Cyber Security Specialist. It is a key reviewing function of Information Governance and Data Security to ensure that IG and GDPR requirements are being demonstrated and embedded across the Trust. The group’s terms of reference are refreshed on an annual basis to develop a work plan to deliver the above duties.

## Training

All staff are required to complete basic information governance, data security and protection training annually, and will also be asked to complete other training commensurate with their duties and responsibilities. Appendix C provides details of the Trust’s training needs analysis conducted by the IG department which is dependent upon the individual’s role responsibilities and function.

Training will be delivered to staff in the following ways:

* Computer Based Training Packages (CBT’s)
* Peripatetic specialist training
* Formal training courses
* External providers

Staff requiring support should speak to their line manager in the first instance. Managers should contact the Corporate IG Services Team if there are specific training needs.

# Section B – IG Policy and Strategic Management Framework

## Introduction

This document sets out the approach to be taken within the Trust to provide a robust Information Governance Framework for the management of information. It supports the Information Governance policy and internal procedures by addressing key areas for Information Governance development across the Trust and with our partners and must not be seen in isolation as information plays a key part in governance, strategic risk, security, knowledge management, service planning, procurement and performance management.

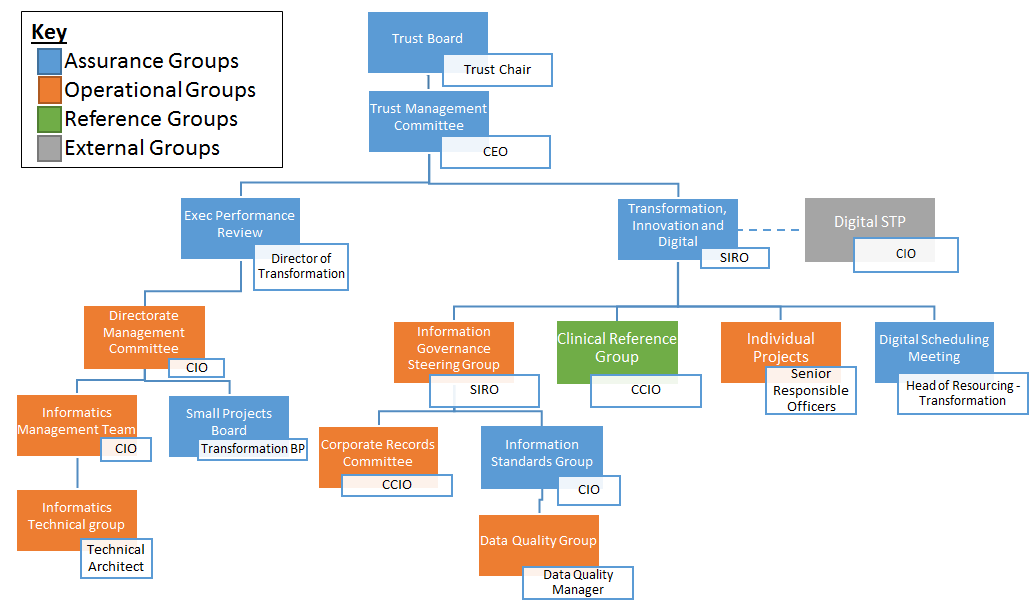
The information governance policy and strategic management framework and procedures are made available to staff via the website and shared drive to improve staff awareness of the Trust’s approach to future Information Governance developments.

* 1. **Key Related Standard Operating Procedures:**
* **Information Asset Management/Security**
  + IG Contract Compliance Assessment
  + Business Continuity
  + Disaster Recovery
  + Third Party/Data Processor Assurance Process
  + Data Flow mapping Procedures
  + Data Protection Impact Assessments
  + Forensic Readiness
  + Audit/Compliance Assessments
  + Registration Authority Smartcard Management
  + Asset Disposal: Equipment, devices, systems, applications
* **Investigations**
  + Forensic Readiness Procedures
  + Procedure to Monitor employee Equipment, Location, Email, Internet, and System and or Application Activity
* **Information Sharing Procedures**
  + 3rd party access to systems and compliance monitoring
  + Incident reporting and investigations
  + How to raise data quality concerns
  + Governance/Liability/Responsibilities
  + Data Transfers
  + Anonymisation and Pseudonymisation Procedures
* **Data Protection, Confidentiality and Security**
* Breach Notification
* Complaints and Concerns
* Information Governance Departmental Compliance Audit
* Clinical Commissioning Audit Procedures
* **Corporate Records Management**
  + Storage and Retrieval of Electronic Corporate Records
  + Retention and Disposal of corporate records
  + Transferring Corporate Records to a local place of deposit ( National Archives)
  + Corporate and Data Quality
  + Audits
  + Email Standards and Procedures
  + Faxing Standards and Procedures (Emergency use only)
  + NHS Mail:
    - Email, SMS Text Messaging and Faxing Standards and Procedures
* Procedures to authorise access a member of staffs emails due to sickness, absence.
* **Freedom of Information**
  + Requests Procedure
  + FOI Complaints
  + FOI Internal Reviews and Public Interest
  + Internal Escalation of Division/Departmental none compliance
* **Healthcare Records Management**
  + Use, Creation and Management of Health Records (paper and electronic)
  + Amendment of Health Records
    - Paper
    - electronic
  + Retention and Disposal of Health Records (paper and electronic)
  + Data Quality Health Records
  + Redaction: Paper and Electronic
* **Access to Healthcare Information**
  + By the patients, representatives, employees and or a member of the public.
  + On behalf of a patient who lacks capacity ( Power of Attorney)
  + Deceased patients
  + Release of Information to the Police, Courts and Other Authorities.

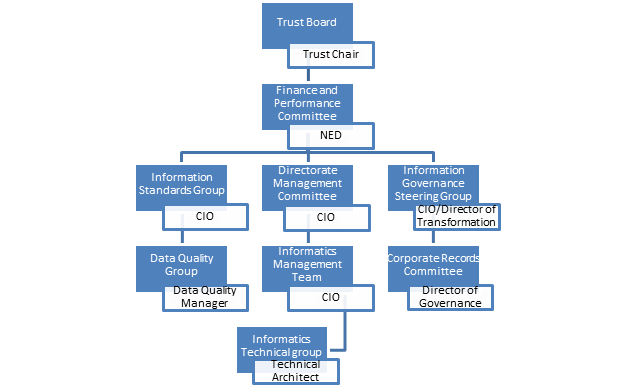
Readers of this policy are required to note that the above list is not exhaustive and reference should always be made to the Information Governance Policy and Procedures Intranet Page to access the most up to gate guidance and documents: <http://ig/>

* 1. The Information Governance Steering Group (IGSG) oversees the Information Governance agenda.
  2. Reporting structures:

## Diagram 1: Overall reporting structure



## Diagram 2: Information Governance reporting structure



* 1. The following organisational resources are available to support the IGSG:
* Medical Director (Caldicott Guardian)
* Director of Transformation (SIRO)
* Chief Information Officer
* Deputy Director of OD and People
* Director of Corporate Governance
* IG/RA Manager/Data Protection/Privacy Officer
* Cyber Security Specialist
* Head of Medical Records
* Information Asset Owners
* Information Asset administrators
* Senior Procurement Manager

## Strategic Aims

The Trust is committed to the following aims to drive forward and improve Information Governance compliance within the organisation.

### Table 3: Strategic Aims

|  |  |  |  |
| --- | --- | --- | --- |
| Aim | Detail | Outcome | Measures |
| **Training & Awareness** | Fundamental to the success of delivering the Information Governance Policy and Strategic Management Framework is developing an Information Governance culture within the organisation. Awareness and Information Governance and Security training is mandatory for all Trust staff through an e-learning programme. The Trust’s training needs analysis (TNA) identify staff roles where additional Information Governance training is required and this is made available through a variety of sources including e-learning and specialist sessions, as required. | All staff are aware of Information Governance legal and national requirements thus reducing the risk of a breach which could result in distress to patients or colleagues or an incident, complaint, claim or adverse publicity for Salisbury. | Incident Reporting  Staff Survey  Complaints  Compliments  Trust wide Training Compliance Reports  Sharing Outstanding Excellence: SOX |
| **Openness & Transparency** | Openness and transparency will be promoted via the Trust’s website and through the proactive publication of patient and staff information, policies and procedures.  Staff and patients are informed of how their information is used.  Below is an example of how the Trust makes privacy information available to patients and staff:   * **Orally** - face to face or when you speak to someone on the telephone * **In writing** - printed letters; media; printed adverts; forms, such as financial applications or job application forms. * **Through signage** - for example an information poster in a public area. * **Electronically** - in text messages; on websites; in emails; in mobile apps: Your Patient Information - Salisbury NHS Foundation Trust and the [Your Data Matters page on the IG Privacy Website](http://ig/your-data-matters/) * **Staff training and awareness -** successful completion of the NHS Digital IG training by employees; staff awareness campaigns, articles and newsletter articles.   The Trust must ensure that staff and patients are made aware of how their information is used and of the importance of checking accuracy of data.  In order to make sure that all are aware of their rights regarding data, there is a paragraph on all clinical letters sent to patients advising them of the Your Information web page.  All employees are made aware of the contents of the web pages and are required to offer information about how their data is collected, used and shared.  Employees are encouraged to check data accuracy to reduce the likelihood of mistakes being made e.g. incorrect identification of similarly named people. | Staff and patients will be informed about the uses of information held about them.  Effective and timely communication will enable the organisation to move forward with technological advances in a transparent and compliant manner. | Audit  Annual notification to the Information Commissioners Office.  IG acceptance testing for new applications, systems and procedures. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Aim** | Detail | Outcome | Measures |
| **Data Security and Protection Toolkit Compliance** | The Trust will continually reassess compliance on an ongoing basis to reflect changes in the Data Security and Protection Toolkit assertions, to re-evaluate the robustness of evidence and to comply with NHS requirements for continuous rather than annual assessments. | The Trust will ensure a proactive Information Governance culture to meet required performance targets. | Audit  Improvement Reports  Compliance Reports  Evidence Reports  The DSPT itself |
| **Risk Management** | Incidents and potential incidents involving information, data and personal or sensitive records are reported, analysed and lessons learned.  Any unforeseen occurrences involving staff or patient personal information or breaches of confidential business information (in whatever format) must be reported in the first instance by the Trust’s Risk Management System ‘Datix’.  If the severity threshold contained within the DSPT Serious Incident Reporting Tool is reached, the incident will be externally reported.  Information Governance incidents may include Information Management Technology and Security, unauthorised access, Caldicott/Data Protection/Freedom of Information or all aspects of records management from creation to disposal.  Employees are encouraged to report these types of incidents promptly and must receive feedback to enable them to improve practice. | Improved incident reporting and hence, better understanding of real and potential risks requiring action. | Compliance Reports |
| **Cyber Essentials Plus** | Secure our Internet connection - firewall  Secure our devices and software - settings  Control access to our data and services  Protect from viruses and other malware  Keep our devices and software up to date | Guard against the most common cyber threats and demonstrate our commitment to cyber security  Less to complete in DSPT | Accreditation by independent certification body |
| **Aim** | Detail | Outcome | Measures |
| **Data Quality** | The Trust will ensure that the data it uses is as accurate and up-to-date as possible.  The Trust has data validation procedures to ensure agreed timescales for correction of errors and omissions. Corrections must be made within a maximum of 6 months. The procedure also includes a requirement to keep staff informed of these issues.  The Trust supports data quality across the directorates to ensure the provision of accurate data to support management and the procurement of patient services.  The Trust ensures robust data quality checks are built in to the introduction and ongoing development of technological solutions to improve and manage records. | Clear procedures around validation checks carried out and improved accuracy of information. | Audit: Internal and External  Compliance Reports  Spot checks |
| Aim | Detail | Outcome | Measures |
| **NHS Number**  (Records Management / Information Lifecycle Strategic Aims) | The organisation will work towards the use of the NHS number in all patient records and documentation related to the direct care of the patient, or where there is legal gateway, or the individual has consented. | The ability to provide safe, urgent and integrated care is fundamental to the future delivery of the health and social care system so that clinicians and patients can have access to the right information at the right time. This needs an underpinning primary identifier across the system - the NHS Number (NHSN). | Destruction Logs  Corporate Records Audit  Information Asset Workstream Reports  External Audit |

|  |  |  |  |
| --- | --- | --- | --- |
| Aim | Detail | Outcome | Measures |
| **Rationalising Records** | All staff will work towards rationalising record collections through sharing records and the information they contain (subject to the requirements of the Caldicott Principles, the General Data Protection Regulation and Data Protection Act 2018, Environmental Information Regulations 2004 and Freedom of Information Act 2000) by merging or ensuring effective cross-referencing.  The Trust will conduct regular audits which look at the records ‘owned’ by the organisation and how they are stored and transferred.  Following each audit, it is possible to identify records (manual and electronic) held by members of staff within. At this point, the Lead in Records Management will be able to determine if any of these records could be subject to record sharing. If it is decided that different systems with common sets of data need to continue, documented procedures must be developed to ensure that any differences between the records are reconciled. Consideration will also be given to whether records could be merged or cross-referenced. The Information Asset Owners will ensure that all records held by their teams are included and assessed as part of the ongoing audits.  All teams across the Trust are responsible for ensuring that they have a manageable and accessible filing system which reduces duplication and avoids retention of files beyond the recommended limits or operational need. | Record collections assessed for rationalisation potential which will in turn reduce duplication and possible errors and effective progress towards integrated records | Audits  Information Asset Work-stream Reports  External Audit |
| Aim | Detail | Outcome | Measures |
| **Records Storage and Maintenance**  (Records Management / Information Lifecycle Strategic Aims) | All manual and electronic records owned by the Trust will be appropriately stored and maintained in accordance with guidance and legislation (see Records Management Procedure).  **Manual Records:** Storage facilities for current paper records are very restricted requiring ongoing review processes to support disposal or long term retention off site. Records must only be kept long term where there is a specific requirement to do so as stated in the NHS Code of Practice: Records Management Retention Schedules.  Any records containing personal data may only be retained in line with the General Data Protection Regulations and UK Legislation which state that data cannot be legally kept for any longer periods without express consent of the identifiable individuals.  **Non-Paper Records:** There must be ongoing review of electronically held data to include retention periods and general housekeeping. General housekeeping issues include deleting duplicates and unnecessary information (whilst following the correct retention periods) from the server or any stand-alone systems. It should also be ensured that all confidential information is stored in the correct sections of the server. | Streamlined approach to paper record retention according to guidelines.  Streamlined recording of electronic data according to guidelines and a reduced risk of information data breaches and ensuring compliance with retention guidelines. | Audit Reports  IAO Information Asset Work stream Reports |

|  |  |  |  |
| --- | --- | --- | --- |
| Aim | Detail | Outcome | Measures |
| **Records Disposal**  (Records Management / Information Lifecycle Strategic Aims) | Records will be reviewed under the retention periods stated and those no longer required by the services of the organisation will be considered for disposal e.g. permanent preservation, long term archiving, transfer, destruction or any other use as agreed by the relevant Line Manager / Data Protection Officer/Caldicott Guardian.  There are occasions when records may need to be passed on to other NHS organisations thus disposing of the record. Detailed audits of such movement of records will be maintained. The principles of Caldicott, Data Protection and the IG Assurance programme must be adhered to.  A record or brief description must be kept about any record that has been destroyed if it is deemed to be a document that was relevant to the business of the organisation. Further guidance should be sought from Corporate Services, if required.  Methods of disposal of records must meet confidentiality and security guidelines. For records disposed of by a contractor, the contractor will be required to sign confidentiality agreements and produce written certification as proof of destruction.  Action will be taken in the event of confidence being breached (e.g. termination of contract) will be specified. This will be managed as part of the organisation’s waste management policies and procedures giving due account to WEEE regulations for electronic equipment and best practice guidance on disposing of computer hardware. |  | Audit Reports and Destruction Logs submitted by departments |
| Aim | Detail | Outcome | Measures |
| **Documentation**  (Records Management / Information Lifecycle Strategic Aims) | Standards will be applied to the production of documentation (manual and electronic) to ensure good record keeping principles are adhered to.  The organisation has professional record keeping standards, staff training and a plan of audits to ensure high standards are maintained.  Corporate standards have been reviewed across the organisation to ensure consistency and a policy and procedure has been developed to inform staff of the model formats for policies, strategies and procedures (Policy on Procedural Documents). Other guidance will be available on the Trust’s Intranet page. | Improved quality control and consistency of records. Improved corporate image and clarity for staff concerning publications / documentation.  Increased understanding of documentation by the general public. | Audit  Spot checks  Document compliance checks conducted during the Freedom of Information Release Process. |

## Openness, Transparency and Information Sharing

* 1. The Trust will ensure that the principles of Caldicott and the regulations outlined in the General Data Protection Regulation and the Trust’s Information Governance Procedure underpin the management of confidential information at all times.
  2. The Trust will ensure individual’s fundamental rights are upheld by informing them about how their information is collected, used, stored, shared and provide them with the option to restrict data sharing where a statutory duty does not exist.

The Trust demonstrates compliance with the EU General Data Protection Regulations (GDPR) and UK legislation using a layered approach, whereby key privacy information is provided immediately, which records the type of information and how it will be used and how long it will be retained for. If appropriate, individuals will be provided with the opportunity to control and object to the use and sharing of their personal data.

Proactive communication with employees is achieved primarily through the cascading of information via the Chief Executive Cascade Brief process, internet and intranet, promotional materials; computer based training (CBT) packages, and face to face training and discussion with patients.

* 1. As a Data Controller, the Trust is obliged to notify the Information Commissioner of the purposes for which it processes personal data. Notification monitoring within the organisation is carried out by the Data Protection Officer. Before the annual review of the Trust’s Notification, the Data Protection Officer will review the types of processing being carried out within the Trust (e.g. from the annual Information Asset Audit) to ensure that the processing complies with the requirements laid down in the General Data Protection Regulations. Individual data subjects can obtain full details of the organisation’s data protection registration/notification with the Information Commissioner from the Information Commissioner's website ([www.ico.gov.uk](http://www.ico.gov.uk)). The Trust’s ICO Registration Number is Z6613850.
  2. The Trust promotes transparency with the public by maintaining and publishing:
* Annual Accounts
* Data Protection Registration with the Information Commissioner’s Office
* Data Security and Protection Toolkit (DSP Toolkit)
* Care Quality Commission (CQC) inspection results
* Privacy Impact Assessments
* Details of Data breaches
* Information relating to national initiatives and guidance
* Responses to freedom of Information Requests
  1. Information Sharing and Collaborative Working

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. As an Acute Trust we need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest. Detailed guidance can be found in the organisation’s Information Sharing Procedure.

As more and more information that affects a business is created and stored elsewhere it is essential to establish how the organisation operates and shares information with stakeholders, partners and suppliers.

Please refer to the Information Sharing Procedures which defines:

* the processes for sharing information with third parties;
* how the organisation can manage how third parties handle personal and confidential information;
* how information governance fits within supplier relationships and contractual obligations;
* measurements and metrics for third parties meeting the Trust’s information governance goals.
  1. Non-confidential information about the Trust and its services is made publically available in compliance with the Freedom of Information Act 2000 and Environmental Information Regulations 2004. The organisation’s Publication Scheme will continue to meet the requirements of the Information Commissioner’s Office Model Scheme for health bodies.
  2. Patients have free access to their own healthcare information. The Trust has laid down clear procedures and arrangements for handling requests for personal information from staff and/or patients, and the public detailed in the organisation’s Access to Records Procedures and Records Management Procedure.

## Information Security

* 1. Information security risk is inherent in all administrative and business activities and everyone working for, or on behalf of, the Trust continuously manages information security risk. The aim of information security risk management is not to eliminate risk, but rather to provide the structural means to identify prioritise and manage risks in a proactive manner. It requires a balance between the potential harm an information breach or loss would cause to the individual, the cost of managing and treating information security risks, with the anticipated benefits that will be derived.
  2. The principles of information security require that all reasonable care is taken to prevent inappropriate access, modification or manipulation of data from taking place. In the case of the NHS, the most sensitive of our data is patient record information. In practice, this is applied through three cornerstones - confidentiality, integrity and availability.

|  |  |
| --- | --- |
| **Confidentiality** | Information must be secured against unauthorised access |
| **Integrity** | Information must be safeguarded against unauthorised modification |
| **Availability** | Information must be accessible to authorised users at times when they require it |

* 1. The Trust undertakes audits or commission assessments of its information and IT security arrangements. Risk assessments will determine appropriate, effective and affordable information security controls are in place.
  2. The Trust will continue to promote effective confidentiality and security practices to its staff through policies, procedures and incorporate it into the IG Training Needs Analysis.
  3. The Trust has in place an incident reporting procedure and will monitor and investigate all reported instances of actual, or potential, breaches of confidentiality and security. Lessons learnt from the investigation will be shared widely throughout the Trust, and recommendations and actions agreed will be performance managed by the Information Governance steering Group.
  4. Information Asset Owners will liaise with the Information Governance department who will collate, on behalf of the SIRO, issues relating to information security risks within their area of responsibility.
  5. An agreement describes the responsibilities of contractors and their sub-contractors under the NHS Confidentiality Code of Practice 2003 and the General Data Protection Regulations when undertaking work for or with the Trust. It must be signed by all contractors prior to entering the Trust site. This is the responsibility of leads managing those contractors, whether they are management associates, or facilities contractors.
  6. A procedure is in place for secure IT asset disposal. Please follow the documented process and contact the Information Governance department for additional information, support or guidance by email: sft.Information.Governance@nhs.net
  7. Staff are reminded that the intentional disclosure of information to a third party where a gain is made for themselves or another, or results in the risk of, or actual loss to NHS or the Trust is a potential criminal offence under Section 4 of the Fraud Act 2006. Suspicion of any such breaches must be reported immediately in accordance with the Trust’s Fraud Policy, or a confidential report can be made to the NHS Fraud & Corruption Reporting Line, by calling 0800 0284060, or Action Fraud on 0300 123 2040.

## Information Quality Assurance/Data Quality

* 1. The Trust has amended the process of reviewing and establishing procedures to support the information quality assurance and the effective management of records. These are to be called the Data Quality Procedure and Records Management Procedure.

There is now (since 2018) a routine assessment of the data quality of all of our regular reporting outputs and metrics against a national DQ framework consisting of 7 standards (Relevant, Timely, Monitored, Complete, Validated, Audited, Reliable). This assures ourselves and the recipients of our reports of the quality of the data that is contained within them and there is a clear schedule of when reporting procedures should be reviewed and if necessary updated. This work is led by the named Regular Reporting Lead for the team. Reporting queries and procedures are reviewed at least annually and any issues found are escalated to the Information Standards Group (ISG) as soon as possible for review. The data quality assessment of our reports occurs at least every two years with the next update scheduled for completion by 1st Jan 2021.

The Deputy Head of information and the DQ Senior Analyst recently completed an online NHS Digital Data Quality Self-assessment checklist (new for 2020) which is a bi-annual recommended requirement, next update due March 2021. This indicates the areas where we can improve DQ in terms of processes, reporting, accountability, oversight etc. The scores and comments are shared with the Information Standards Group and the results are incorporated into the DQ Implementation timeline which has been extended to a new deadline of 31st March 2021 in recognition of the impact of COVID-19 on delivery. The recruitment of a full time Data Quality Manager will further reinforce the Data Quality policy, associated DQ procedures and drive the implementation of the new DQN app which will better inform users around the Trust of DQ errors that they are making in order that information is inputted correctly into the Trust’s various information systems at the earliest opportunity. This post is currently being advertised with the current post holder’s secondment due to end in Jan 2021.

* 1. Audits will be undertaken or commissioned of the organisation’s quality of data and records management arrangements. The results of the audit will be scrutinised by the members of the Audit Committee and Information Governance Steering Group (IGSG).
  2. Wherever possible, information quality will be assured at the point of collection. Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended. Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

## Data Protection

* 1. The Trust collects, stores, and processes information about its employees, patients and other individuals for a variety of purposes (for example, the provision of healthcare services or employment which requires correspondence and communication). To comply with the Data Protection Act 2018 and EU General Data Protection Regulation (GDPR) information must be collected openly and transparently, used fairly, held in an identifiable format for no longer than necessary, stored safely, and not disclosed to any unauthorised person. The Act and Regulation applies to manual and electronic records. The lawful and correct treatment of personal information is vital to successful operations, and to maintain confidence within the organisation and the patients it treats.

The Trust will comply with the requirements of the GDPR by incorporating the six data protection principles within the organisations internal policies, processes and procedures. Table 4 below, lists the GDPR requirements which must be met by data controllers:

### Table 4: Six Data Protection Principles

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Data Protection Principle** | | **Expectation** |
| **1** | processed lawfully, fairly and in a transparent manner in relation to individuals | The Trust must ensure that its internal processes and procedures governing the collection and use of personal data explain why it is being collected, what it will be used for, how long it will be stored and how they can receive copies of the information held | |
| **2** | used for limited, specifically stated purposes | collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes; | |
| **3** | Using the minimum amount necessary | adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; | |
| **4** | Accurate | accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, and are erased or rectified without delay; | |
| **5** | kept in an identifiable format no longer than necessary | kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; | |
| **6** | Securely | processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.  requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used. | |

* 1. Individual’s Rights

Under the Human Rights Act individuals have the right to a private life without interference from the state (country) or another individual.

Private life has a broad meaning. It means you have the right to live your life with privacy and without interference by the state. It covers things like:

* A person’s sexuality;
* their body;
* personal identity and how you look and dress;
* forming and maintaining relationships with other people;
* how personal information is held and protected.
  1. Individuals’ rights under the General Data Protection Regulations (GDPR)

Table 5 below contains the details of the six data protection principles and the legal expectations the Trust is required to achieve in order to comply with GDPR.

### Table 5: GDPR principles and expectations

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Data Protection Principle** | | **Expectation** |
| **1** | Information is processed lawfully, fairly and in a transparent manner in relation to individuals | The Trust must ensure that it internal processes and procedures governing the collection and use of personal data explain why it is being collected, what it will be used for, how long it will be stored and how they can receive copies of the information held | |
| **2** | Information is used for limited, specifically stated purposes | collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes; | |
| **3** | Using the minimumamount necessary | adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; | |
| **4** | Information is accurate | accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; | |
| **5** | Information is kept in an identifiable format no longer than necessary | kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; | |
| **6** | Information is Secure | processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.  requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used. | |

* 1. **Data Protection Officer/Information Governance Manager**

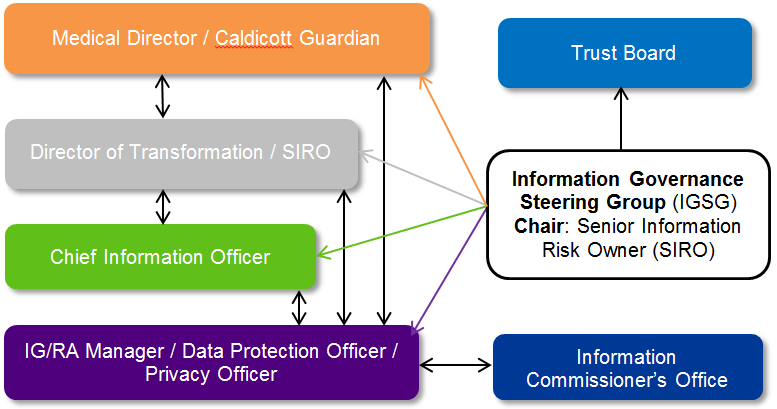
Under the General Data Protection Regulations (GDPR), public authorities are required to appoint a Data Protection Officer (DPO) who must report to the highest management level of the organisation. They must operate independently and cannot be dismissed or penalised for their task. Adequate resources must be provided to enable the DPO to meet their GDPR obligations.

* + 1. Tasks of a Data Protection Officer

The data protection officer role within the Trust includes the following tasks:

* to inform and advise the controller or the processor, and the employees who carry out processing, of their obligations pursuant to this regulation and to other Union or Member State data protection provisions;
* to monitor compliance with this regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
* to provide advice where requested as regards the data protection impact assessment and monitor its performance;
* to cooperate with the supervisory authority - Information Commissioner’s Office;
* to act as the contact point for the ICO on issues relating to processing, and to consult, where appropriate, with regard to any other matter.
* The data protection officer shall in the performance of their tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.
* Submission of the Data Security and Protection Toolkit
* To provide support advice and guidance to the Caldicott Guardian and SIRO on information sharing, confidentiality and security.
* To provide support, advice and guidance to the CEO with Freedom of Information (FOI) request compliance.
  + 1. Data Protection Officer/IG Manager’s Accountability Framework

Diagram 3 - Data Protection Officer/IG Manager’s Accountability Framework belowillustrates the internal multifunctional reporting, escalation and accountability framework for data protection within the Trust.



## Confidentiality

* 1. The Common Law duty of confidentiality

Common Law is also referred to as ‘judge-made’ or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider’s consent.

In practice, this means that all patient/client information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed to a non-health/social care professional or administrator unless there is a legal gateway permitting the disclosure.

The common law duty of confidence is maintained within a healthcare setting by ensuring personal and special categories of personal data are stored in secure locations and role based access controls and audit trails protect the confidentiality, integrity and availability of the information on a need to know basis.

* 1. The Caldicott Guardian Responsibilities

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. Each NHS organisation is required to have a Caldicott Guardian; this was mandated for the NHS by Health Service Circular: HSC 1999/012.

At procedural level, the Guardian role is to ensure that those policies and procedures which impact upon the accuracy, management, confidentiality, sharing and retention of the patient record are in place; where they are not, the Guardian must ensure that they themselves play a key role in actively promoting plans to enable this work to be done. The Guardian must ensure that functional responsibility is appropriately delegated; that lines of reporting and responsibility are clear; that sufficient training is given and that there are regular reports to the Board.

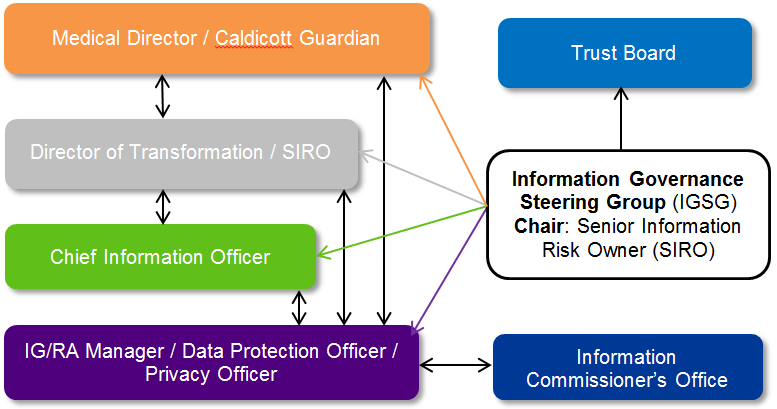
The Trust’s Medical Director is the Trust’s designated Caldicott Guardian. It is their duty to oversee the Caldicott function. This role’s primary concern is upholding and supporting patient confidentiality and ensuring healthcare data is shared appropriately and legally to support patient care pathways across the organisation.

This function is based within the broader remit of the Information Governance Assurance Framework as outlined by the Department of Health’s guidelines. Under the General Data Protection Regulation and other relevant legislation, the role of the Caldicott Guardian is vital in the assurance and safety of patient identifiable information. A national Register of Caldicott Guardians is available to the public on the following website: <https://www.gov.uk/government/groups/uk-caldicott-guardian-council>

The Caldicott annual work plan is conducted by the completion of the new NHS Digital Data Security and Protection Toolkit, an online self-assessment tool which allows organisations to measure their performance against the National Data Guardian’s 10 data security standards recommended by the Dame Fiona Caldicott following an extensive public consultation.

* 1. The Caldicott Guardian Accountability and Organisational Framework

Diagram 4 - Caldicott Guardian Accountability and Organisational Framework below illustrates the internal multifunctional Caldicott reporting, escalation and accountability framework within the Trust.



* 1. The Seven Caldicott Principles

In any case where confidential information has been requested for nonmedical purposes, the Caldicott Guardian will assess whether the information request is supported by the following seven Caldicott principles:

### Table 6: Caldicott Principles

|  |  |
| --- | --- |
| **No** | **Caldicott Principles** |
| **1** | Justify the purpose(s) for using confidential information. Every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed. |
| **2** | Only use information when absolutely necessary. Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. |
| **3** | Use the minimum information that is required. Where use of personal confidential data is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out. |
| **4** | Access to information should be on a strict need-to-know basis. Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes. |
| **5** | Everyone must understand his or her responsibilities. Action should be taken to ensure that those handling personal confidential data are made fully aware of their responsibilities and obligations to respect patient confidentiality. |
| **6** | Understand and comply with the law.  Every use of personal confidential data must be lawful. |
| **7** | The duty to share information can be as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies. |

## Information Risk Management Framework

Information Risk is inherent in the Trust’s activities and an information risk assurance process is set out as a requirement of the Data Security and Protection Toolkit. Information risk management is the ongoing process of identifying information risks and implementing plans to address them. The responsibilities, definitions, processes and templates as contained in the Risk Management Policy & Procedure also apply.

The Trust maintains an Assurance Framework which covers strategic risks, and a Risk Register which covers operational risks. All risks are reviewed regularly by the risk lead in line with the organisation’s Risk Management strategy, policy and procedure Information Governance risks are routinely reviewed on behalf of the Trust Board by the Information Governance Steering Group (IGSG), and escalated via the Trust’s Senior Information Risk Owner (SIRO).

* 1. Senior Information Risk Owner (SIRO) Responsibilities

The Senior Information Risk Owner (SIRO) acts as an advocate for information risk on the Governing Body. The role of SIRO has been incorporated into the role of the Director of Transformation whose primary role is to strengthen information security assurance controls and functions within the Trust, and to provide the Trust board with an annual assurance assessment of security risks.

The SIRO is responsible for leading and fostering a culture that values, protects and uses information for the success of the company and benefits its patients and employees. Ensuring that information asset audits are conducted on a regular bias and, where appropriate, action is taken to minimise potential and perceived risks.

Additional duties include but are not limited to ensuring that:

* The Trust has a plan to achieve and monitor the right culture, across the Trust and with its business partners
* Applicable recommendations made by the Department of Health, NHS Digital relating to information security are adopted.
* They maintain a sufficient knowledge and experience of the organisation’s business goals with particular emphasis on the use of, and dependency upon, internal and external information.
* Information Asset Owners (IAOs) understand their roles and are supported by the information risk management specialists that they need.
* Good information security assurance practice is shared within the organisation and to learn from good practice developed and practiced within other NHS organisations locally and nationally.

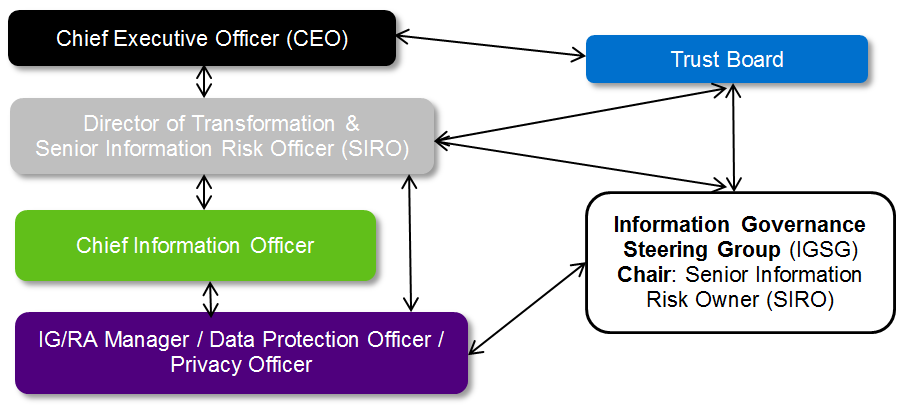
A SIRO must attend and successfully complete an accredited training course endorsed by NHS Digital and NHS England and thereafter complete and pass the relevant NHS Digital e-learning package successfully on an annual basis.

The SIRO is advisor to the Chief Executive and the Trust Board on information security and risk management strategies and provides periodic reports and briefings on progress.

* 1. Senior Information Risk Owner Accountability Framework

The Chief Executive is required to cover information risk in the annual Statement of Internal Controls. Recommendation 2 of NHS Connecting for Health’s data sharing report section stated ‘We further recommend that as a matter of best practice, companies should review at least annually their systems of internal controls over using and sharing personal information and they should report to shareholders that they have done so’.

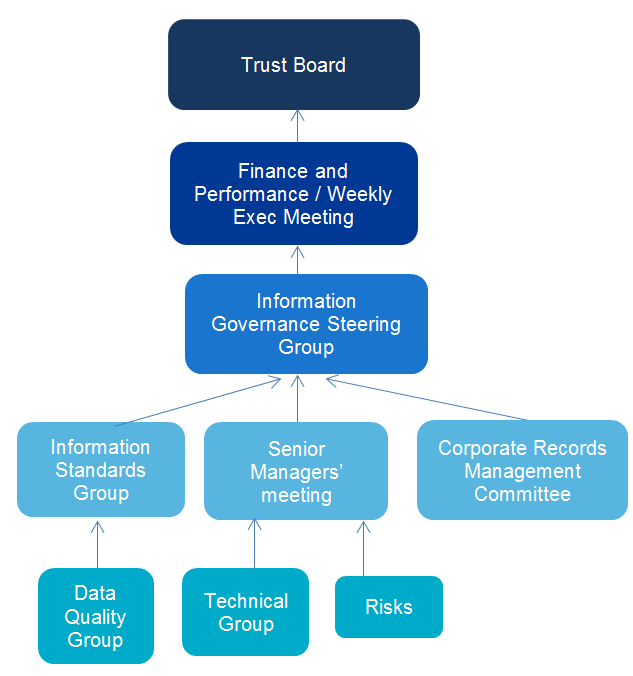
Diagram 5 - Senior Information Risk Owner Accountability Framework illustrates the accountability and communication framework between the Chief Executive Officer, SIRO, Chief Information Officer and the Data Protection Officer, providing assurance and escalation compliance relating to information and security risk management and organisational oversight.



Senior Management Teams identify and collectively manage risks on behalf of the Board. Directors manage information risks within their Directorates, supported by the designated Information Asset Owners and Information Asset Administrators.

The Trust Board, Audit Committee and Information Governance Steering Group (IGSG) receive an annual report on information governance compliance at three key stages within the financial year.

### Diagram 6 - Chief Information Officer – DPST assurance / escalation / sign off process



* 1. Information Risk Management Strategy

It is the objective of the Trust to ensure information risk management is integrated into the Trust’s Information Governance Policy and Strategic Management Framework to ensure compliance with legal, statutory, and NHS Policy requirements which mandate personal identifiable information, systems assets; property and reputation are appropriately managed and safeguarded.

This will be achieved by collating and reviewing risk assessments, analysing and responding to security threat notifications issued by NHS Digital (Care CERT Alerts), which are supported by appropriate action plans, all of which are supported by the IG department through proactive and reactive audits which are scrutinised and reviewed by the IGSG members.

* 1. Managing Information Security Risks

The Trust faces many types of risk - internal, external, strategic and those arising from projects or major Government initiatives. The Information Governance Steering Group proactively monitors information risk reviewing information asset risks, Data Privacy Impact Assessments (DPIAs), cyber security and ransomware reports, incidents, complaints together with internal and external audits.

Information/security risks are overseen by the Trust Director of Transformation/Senior Information Risk Owner on behalf of the Trust Board who is collectively accountable for information risk management and has a collective responsibility to ensure that Boards provide, review, challenge and support the management of risks.

* + 1. Information Risk Assessments

Information risk assessments will be performed on a regular basis for all information systems and critical information assets. Information Risk assessments will also occur at the following times:

* At the inception of new systems, applications and facilities that may impact the assurance of the Trust and or its systems;
* Before enhancements, upgrades, and conversions associated with critical systems or applications;
* When NHS policy or legislation requires risk determination;
* When the Trust’s Executive Management team requires it.
  1. Information Governance and Security Incidents

An Information Governance Incident is an event which may result in:

* Degraded system integrity e.g. causing a virus to enter the system;
* Loss of system availability, e.g. clinical systems not working;
* Disclosure of confidential information e.g. password or smartcard sharing (accidentally or on purpose);
* Disruption of activity e.g. inappropriately deleting files from a network drive.
* Loss e.g. theft of laptop, mobile phone or table;
* Legal action e.g. inappropriate disclosure of patient information
* Unauthorised access to applications e.g. unauthorised access to Lorenzo or the payroll system.
  + 1. Information Governance Incident Management

All Information Governance incidents will be formally logged, categorised by severity and analysed in accordance with the organisation's Incident Management Policy and the NHS Digital Information Governance Serious Incidents Requiring Investigation (SIRI) Procedures.

One or more of the following individuals must also be advised according to the severity and type of incident as appropriate:

* Caldicott Guardian (Medical Director)
* Senior Information Risk Owner (Director of Transformation)
* Chief Information Officer
* Data Protection Officer (IG Manager)
  + 1. Major System Outages and Confidentiality Breach Escalation Procedures

In the event of major breaches of confidentiality, including theft or loss of medical records and electronic equipment containing patient/personal data these must be reported to the Data Protection Officer as soon as possible, and within a maximum of 24 hours in line with Serious Incident (SI) reporting requirements.

Under GDPR, the Data Protection Act 2018, and the Network Information Systems Directive (NIS) the Trust is legal required to send notification to the ICO via the Data Security and Protection Toolkit within 72 hours.

* + 1. Learning from Incidents

Learning from risks, incidents and other such events is vital when developing a culture in the Trust that welcomes the opportunity to improve patient care, and the security and confidentiality of personal information offered by the Trust to ensure the working environment and safety of employees.

All serious Information Governance incidents and results of incident investigations / root cause analyses will be discussed by the Information Governance Steering Group at the earliest subsequent meeting. The SIRO will keep the Board informed as appropriate. Relevant reporting will be made externally in line with Information Governance requirements.

## Information Asset Management

Information Asset Management is central to the efficient running of departments i.e. service user, finance, stock control, paper records etc. Information Assets will also include the computer systems, network hardware and software which are used to process this data.

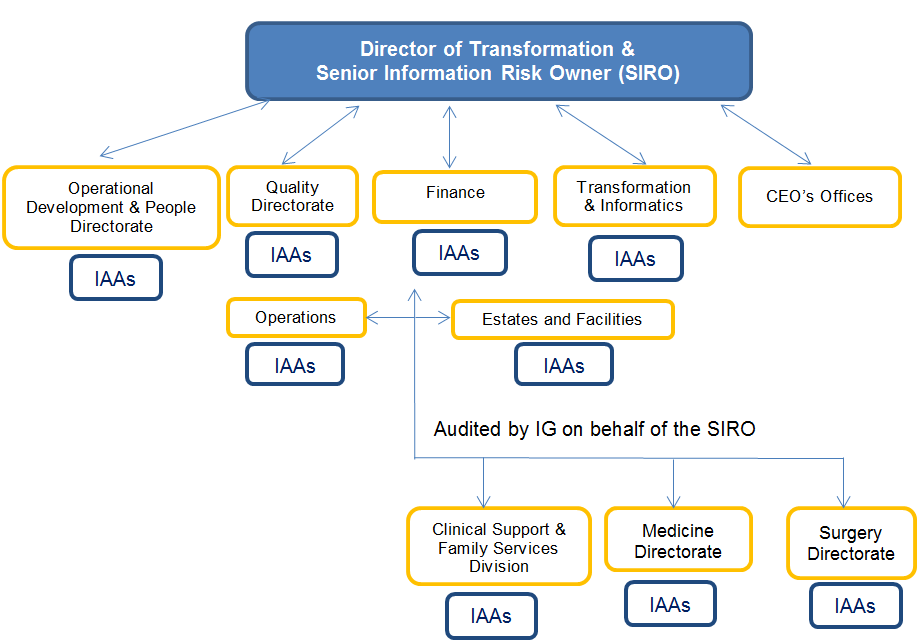
Non-computerised systems holding information must be asset registered with relevant file identifications and storage locations.

### **Table 7: The six main categories of information asset**:

|  |  |  |
| --- | --- | --- |
| **1** | **Information** | databases, system documentation and procedures, archive media and data |
| **2** | **Software** | application programs, systems, development tools and utilities |
| **3** | **Physical** | infrastructure, equipment, furniture and accommodation used for data processing including paper and electronic records |
| **4** | **Services** | computing and communications, heating, lighting, power, air conditioning used for data processing |
| **5** | **People** | qualifications, skills and experience in the use of information systems |
| **6** | **Other** | the reputation and image of the Trust. |

* 1. Information Asset Risk Management Assurance Framework

### Diagram 7 - internal information risk management reporting accountability framework



* 1. Information Asset Owners

The Director, Directorate or Departmental Managers are the Trust’s IAOs. They ensure that information risk assessments are performed annually on all information assets for which they have been assigned ‘ownership’. IAOs submit the risk assessment results and associated mitigation plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans include specific actions with expected completion dates, as well as an account of residual risks and foster an effective IG culture for staff and others who access or use their Information Assets to ensure individual responsibilities are understood, and that good working practices are adopted in accordance with the Trust policy.

Information Asset Owners provide the SIRO with an annual written risk assessment for each information asset ‘owned’ by them.

The IAO ensure each information asset ‘owned’ by them has an assigned Information Asset Administrator (IAA).

IAOs will work closely with other IAOs of the organisation to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. This is especially important where information assets are shared by multiple parts of the organisation. IAOs will support the organisation’s Senior Information Risk Owner (SIRO) in their overall information risk management function.

The IAO is expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals. The IAO will therefore document, understand and monitor:

* What information assets are held, and for what purposes;
* How information is created, amended or added to over time;
* The security of information held within information assets;
* Who has access to the information and why.

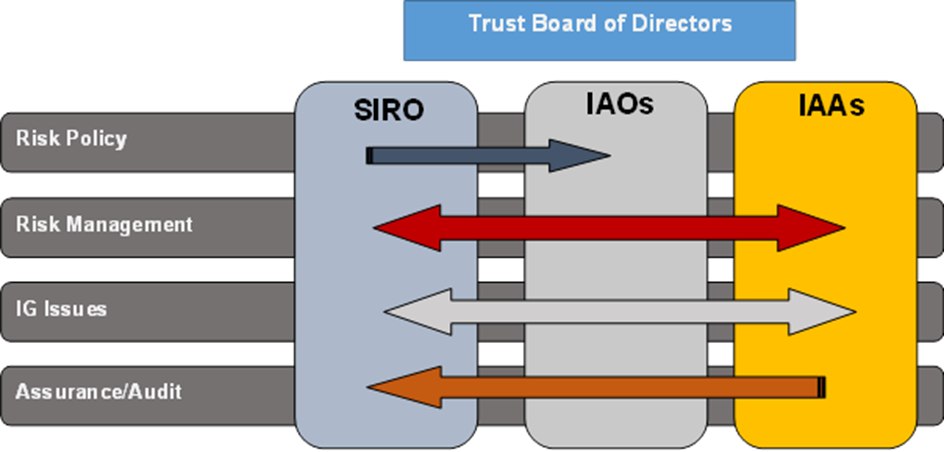
The IAO shall undertake annual training as necessary to ensure they remain effective in their role.

* + 1. IAO Responsibilities:
* Maintenance of an up-to-date and accurate Directorate System Asset Register (SAR);
* Identification and nomination of appropriately skilled individuals to undertake the role of IAA for each Information Asset within their Directorate;
* Add the responsibilities of the IAA to the job description of the individual nominated;
* Take ownership of their local control, risk assessment and management processes for the information assets they own. This includes the identification, review and prioritisation of perceived risks and oversight of actions agreed to mitigate those risks. The IAO is to ensure that the information risks of each asset owned are assessed/reviewed at least annually and where appropriate escalated to the SIRO;
* Provide support to the organisation’s SIRO and IG Lead to maintain their awareness of the risks to all Information Assets that are owned by the organisation and for the organisation’s overall risk reporting requirements and procedures. The IAO is to provide the SIRO with an annual written report on the assurance and usage of each asset owned. This can be achieved via continual maintenance of and annual sign off of the Directorate SAR;
* To ensure that a record of processing activities under their control is maintained and the legal basis for the processing of personal data is recorded and maintained;
* Ensure that staff and relevant others are aware of, and comply with, expected IG working practices for the effective use of Information Assets. This includes records of the information disclosed from an asset, where this is permitted.
* Provide a focal point for the resolution and/or discussion of risk issues affecting their Information Assets.
* Conduct a Data Privacy Impact Assessment (DPIA) for any new or amended project/process/systems/facilities where personal data is to be processed.
  + 1. IAO Reporting Responsibilities

Information Asset Owners are responsible for providing assurance to the SIRO that assets under their control are being appropriately managed, and any risks identified are recorded and escalated.

The diagram below shows and illustrates the communication and reporting relationship between the SIRO, IAOs and IAAs.

### Diagram 8 – Communications SIRO, IAO, IAA



* 1. Information Asset Administrators

An Information Asset Administrator (IAA) will most often be an operational manager or system administrator who is familiar with information risks in their area or department e.g. Security Managers, Records Managers, Internal Audit, or Department Heads.

They will be assigned risk and information management responsibilities for one or more of the organisation’s information assets by the IAO. To prevent possible misunderstandings, IAAs **are not necessarily the end-users** of an information asset.

Responsibility for Information Asset Management and task should appear in the employee’s job description.

* + 1. IAA’s Responsibilities

IAA responsibilities are to:

* **Implement** the organisation’s policies
* **Understand and address risks** to information assets, and provides assurance to the IAO
* **Ensure** compliancewith the organisation Information Risk & Security Policy within their area or department
* **Co-ordinate** and contribute to risk assessments and mitigation implementation
* **Provide** information and reports to the IAO tomaintain relevant parts of the Directorate System Asset Register
* **Maintain** an accurate and up to date record of all users for the information asset for which they are responsible, including a record of all user access levels and the timely reporting of discrepancies to the IAO
* **Ensure** that the organisation’s requirements for information incident identification, reporting, management and response are followed. This includes the mechanisms to identify and minimise the severity of an incident and the points at which assistance or escalation may be required.
* **Ensure** records are appropriately destroyed or archived when an information asset is decommissioned.
* **Assist** the Information Governance Department by completing Asset Audits within a timely manner and making documentation available for review.
  + 1. IAA’s annual tasks/duties (Confirmation of completion must be reported to the IAO):

IAAs are required on an annual basis to:

* Audit and review all users’ access levels, to ensure staff leavers and departmental movers access is revoked, if appropriate.
* Maintain and test a suitable business continuity/disaster recovery plan for their information asset;
* Work with the Procurement Department to review the assets contract to ensure to ensure Information Governance compliance and take remedial action where necessary;
* Maintain and review a map of all flows of personal data to and from the information asset, highlighting any high risks by adding a risk assessment to the Trust Datix system;
* Complete annual information risk management training.
* Undertake an assessment of the business importance/criticality of the asset to the Trust.
* Record and maintain asset risks scoring over 8 within Datix (the Trust’s Risk Management System).
* Record and escalate issues relating to asset performance, details of when the system or application will become end of life. Together with information relating to system outages, unreliability, complaints, concerns, data corruption or information security concerns.

## Data Management

The Trust is committed to maintaining the confidentiality, integrity, quality and availability of its patient services through effective through the data management lifecycle from collection through to destruction. This includes establishing processes to ensure that information assets are formally managed and that data produced can be trusted and relied upon for decision making and service redesign.

**Image 1** right, provides a pictorial view of lifecycle of data management within the Trust.

Information lifecycle management recognises that the value of information changes over time and must be managed accordingly. The process classifies information to its business value and establishes policies to migrate and store information. It also reduces the risk of retaining unneeded information which has reached its maximum retention schedules in line with the [Records Management Code of Practice for Health and Social Care 2016](https://digital.nhs.uk/binaries/content/assets/legacy/pdf/n/b/records-management-cop-hsc-2016.pdf): Retention Schedules: <https://digital.nhs.uk/binaries/content/assets/legacy/excel/o/o/rmcop-retention-schedules.xls>

The proactive archiving and management of information can reduce information security risks and storage costs associated with personal information held in retired obsolete systems and paper format.

## Information Technology (IT) Asset Management

IT asset management is a set of business practices which join financial, contractual, and inventory function to support the life cycle management and strategic decision making for the Trust. It allows the Trust to get the maximum value and benefit from the system, equipment or application.

To provide assurance to the Trust Board, Senior Information Risk Owner (SIRO) and Information Governance Steering Group (IGSG), the following IT asset management process has been introduced to ensure the Trust holds a comprehensive list of:

* What systems, applications and hardware exist
* The legal basis for collecting the information
* The secondary purposes for which the information is used
* Its primary purpose of function
* The sensitivity of the personal data held
* How the system is used
* How much it cost
* Resources required to support the system
* When they are coming up for renewal or upgrade
* When it require security and patching updates
* How they impact on IT and business services
* How long it will be retained
* When they will be decommissioned.

**Image 2** right, provides a pictorial view of IT asset lifecycle management which starts at the planning and purchasing phase, then acquiring the product, which naturally evolves into deployment, management (business as usual) and eventually the retirement, archiving and disposal.

Compliance with the IT asset lifecycle management will be monitored through the procurement process controls, internal and external audit reports, the monitoring of reconciliation and asset disposal procedures.

## Freedom of Information and Environmental Information Regulations 2000

* 1. The Freedom of Information Act 2000 is part of the Government’s commitment to greater openness in the public sector.

The main features of the Freedom of Information Act are:

* A general right of access from 1st January 2005 to recorded information held by public authorities, subject to certain conditions and exemptions;
* In cases where information is exempt from disclosure, except where an absolute exemption applies, a duty on public authorities to:
  + Inform the applicant whether they hold the information requested, and
  + Communicate the information to him or her, unless the public interest in maintaining the exemption in question outweighs the public interest in disclosure;
* A duty on every public authority to adopt and maintain a Publication Scheme, specifically applicable to the NHS from 31st October 2003;
* The office of the Information Commissioner with wide powers to enforce the rights created by the Freedom of Information Act and to promote good practice;
* A duty on the Lord Chancellor and Information Commissioner’s Office to disseminate Codes of Practice for guidance on specific issues.

As a public body, the Trust is obliged to respond to all FOI requests for information within 20 working days. The process is managed at SDH by the Information Governance team who record and send requests for information to the Information Guardians within the Trust. The Information Guardians then contact staff within their area/directorate/team for the detail requested and relay the answers to questions back to the IG team. This is then forwarded to the CEO, or deputy, for review and authorisation to send.

With such a short timeframe, it is vital that all staff answer any queries as quickly as possible so that the Trust is not in breach of its obligations. All FOI responses are published on the main hospital website. <http://www.salisbury.nhs.uk/AboutUs/FreedomOfInformation/Pages/Home.aspx>

* 1. Environmental Regulations 2004

The Environmental Information Regulations 2004 give rights of public access to environmental information held by public authorities. These regulations have been introduced in line with European Directive 2003/4/EC and the Aarhus Convention on Access to Information, Public Participation in Decision Making and Access to Justice in Environmental Matters 1998.

The Environmental Impact Regulations 2004 permit exceptions rather than exemptions and the emphasis is in favour of disclosure. It is important for the Trust to make the distinction between Freedom of Information and Environmental Information Regulations and to respond accordingly.

The Trust believes that as a public authority it must be allowed to discharge its functions effectively. This means that the Trust will use the exemptions contained in the Freedom of Information Act 2000 where an absolute exemption applies or where a qualified exemption or exception can reasonably be applied in terms of the public interest of disclosure. Detailed information can be found in the Freedom of Information and Environmental Information Regulations standard operating procedures.

## Records Management / Information Lifecycle Management

The Trust recognises the need to ensure a structured and integrated approach to Records Management throughout the organisation, which supports the overall information governance arrangements within the organisation.

The Trust is committed to a systematic and planned approach to the Management of Records, from their creation to their ultimate disposal in accordance with relevant legislation. This will ensure that the Trust can control both the quality and quantity of the information that it generates, it can maintain that information in an effective manner, and it can dispose of efficiently in accordance with the NHS Code of Practice: Records Management Retention Schedules when no longer required. Detailed Records Management guidance can be found in the Records Management Procedures.

The Corporate Records Management Committee will follow the Designing Record Keeping Systems Design and Implementation of Record Keeping Systems (DIRKS). The industry standard for the design and implementation of record keeping systems, as given in the ISO standard ISO15489-1:200131, is an eight stage process that can be summarised as:

1. Conduct preliminary investigation

2. Analyse business activity

3. Identify requirements for records

4. Assess existing systems

5. Identify strategies to satisfy requirement

6. Design records system

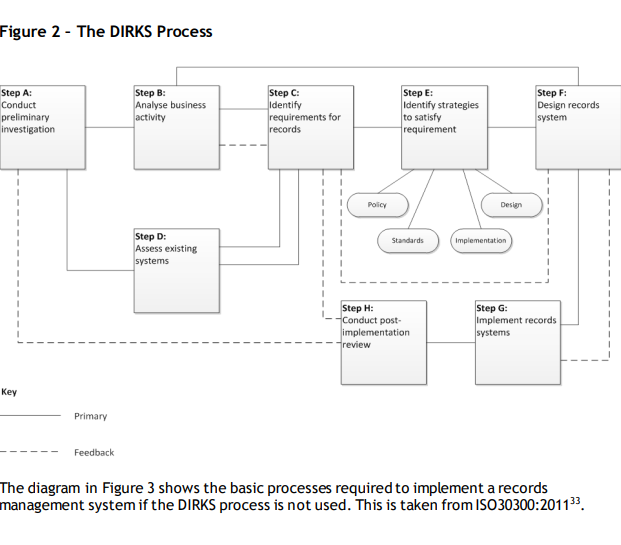
7. Implement records systems

8. Conduct post implementation review.

Figure 2 indicates the relationship of the stages. Further details can be sought from the ISO standard and supplementary guidance. In addition to the stages outlined above, a privacy impact assessment must also be conducted where necessary. For more advice and information please see the Information Commissioner’s Office (ICO) Privacy Impact Assessment Code of Practice

This has been revised in ISO15489-1:2016 and will be evaluated and the Code updated where necessary at the next revision. Early indications are that changes are presentational as opposed to material. 32 ICO Privacy Impact Assessment Code of Practice <https://ico.org.uk/media/fororganisations/documents/1595/pia-code-of-practice.pdf>

There are a series of other British and international standards that are used to produce record keeping systems. For details of the standard making bodies, please see Appendix Two. These all interrelate and work within the same guiding principles and where possible use the same terminology. They all rely upon defining roles and responsibilities, processes, measurement, evaluation, review and improvement. Figure 2 – The DIRKS Process The diagram in Figure 3 shows the basic processes required to implement a records management system if the DIRKS process is not used. This is taken from ISO30300:201133.



## Improvement Plan and Assessment

Assessments of compliance with each requirement within the Data Security and Protection Toolkit (DSPT) will be undertaken throughout each year. Annual reports and proposed action / development plans will be presented to the Information Governance Steering Group for approval prior to submission annually in March.

The Data Security and Protection Toolkit is an online self-assessment tool that permits the Trust to measure its performance against the National Data Guardian 10 Security Standards listed below:

1. Personal Confidential Data
2. Staff Responsibilities
3. Training
4. Managing Data Access
5. Process Reviews
6. Responding to Incidents
7. Continuity Planning
8. Unsupported Systems
9. IT Protection
10. Accountable Suppliers

## Employee and Managers’ Handbooks: Your Roles and Responsibilities for IG

The strategy and framework covers all staff, contractors and students that create, store, share and dispose of information. It sets out the procedures for sharing information with stakeholders, partners and suppliers. It concerns the management of all paper and electronic information and its associated system repositories regardless of location that affects its regulatory and legal obligations.

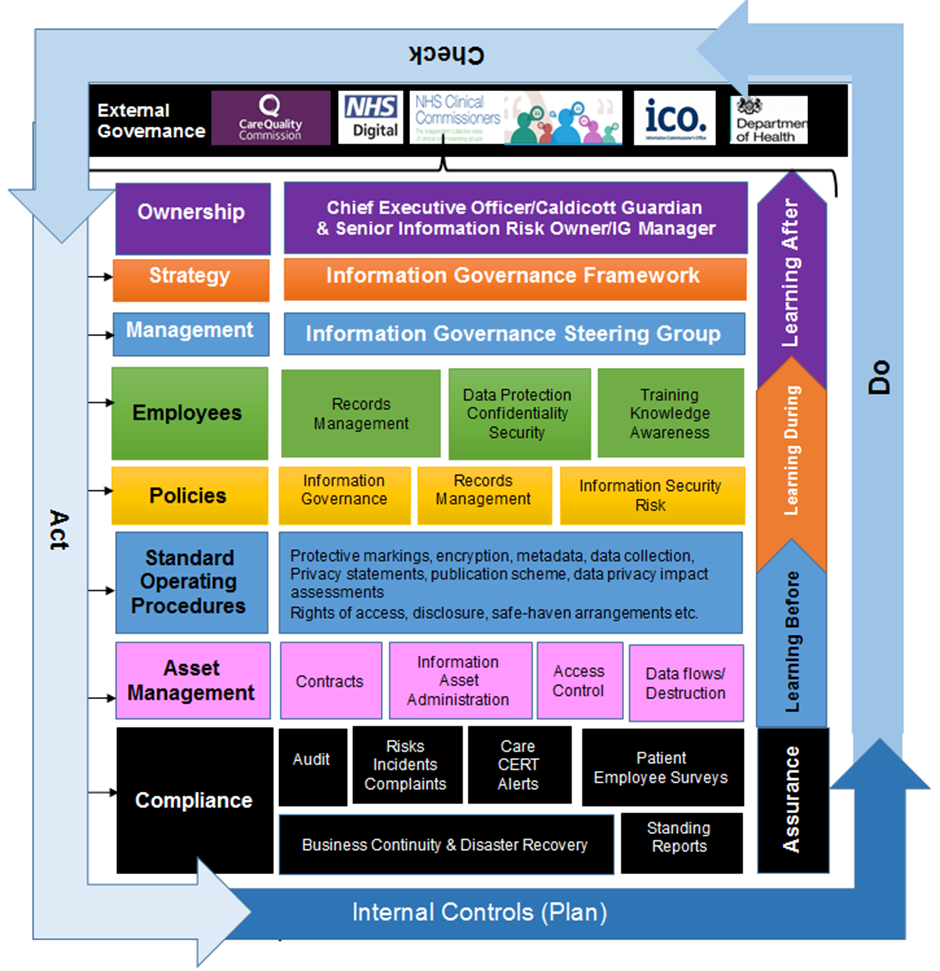
It is the responsibility of Executive Directors, Division/Clinical Managers, Senior Clinicians, Heads of Departments, Divisional Senior Nurses, Matrons and Ward Sisters/Charge nurses to ensure the implementation of policies throughout their areas of responsibility. Managers must also react in an appropriate manner when informed of instances where behaviour is not in accordance with this framework set out herein. Managers are responsible for engaging with a Guardian of the Corporate Records Management Committee to ensure that the outcomes are completed. There is also an overview showing the specific role and responsibilities for the Corporate Records Management Committee Guardians at Appendix G.

A staff handbook has been developed to help all staff understand their roles and responsibilities around information governance across the Trust Appendix A. This will be sent electronically to all new starters with their contract of employment. There is also a handbook showing the specific additional IG responsibilities for managers at Appendix B.

# Section C – IG Standard Operating Procedures

Diagram 9 - Internal and External Information Governance, Data Protection, Confidentiality, and Security Assurance Framework

This is supported by the Plan, Do, Check; Act approach which aims to achieve a balance between the systems and behavioural aspects of information management as an integral part of good management generally, rather than as a stand-alone system.



# Appendices

A: Employee IG Handbook (top document in IG guidance documents) – [link to document](http://ig/policies-procedures-and-guidance/)

B: Manager’s IG Handbook (second document in IG guidance documents) – [link to document](http://ig/policies-procedures-and-guidance/)

C: IG Training Needs Analysis for 2018-2020

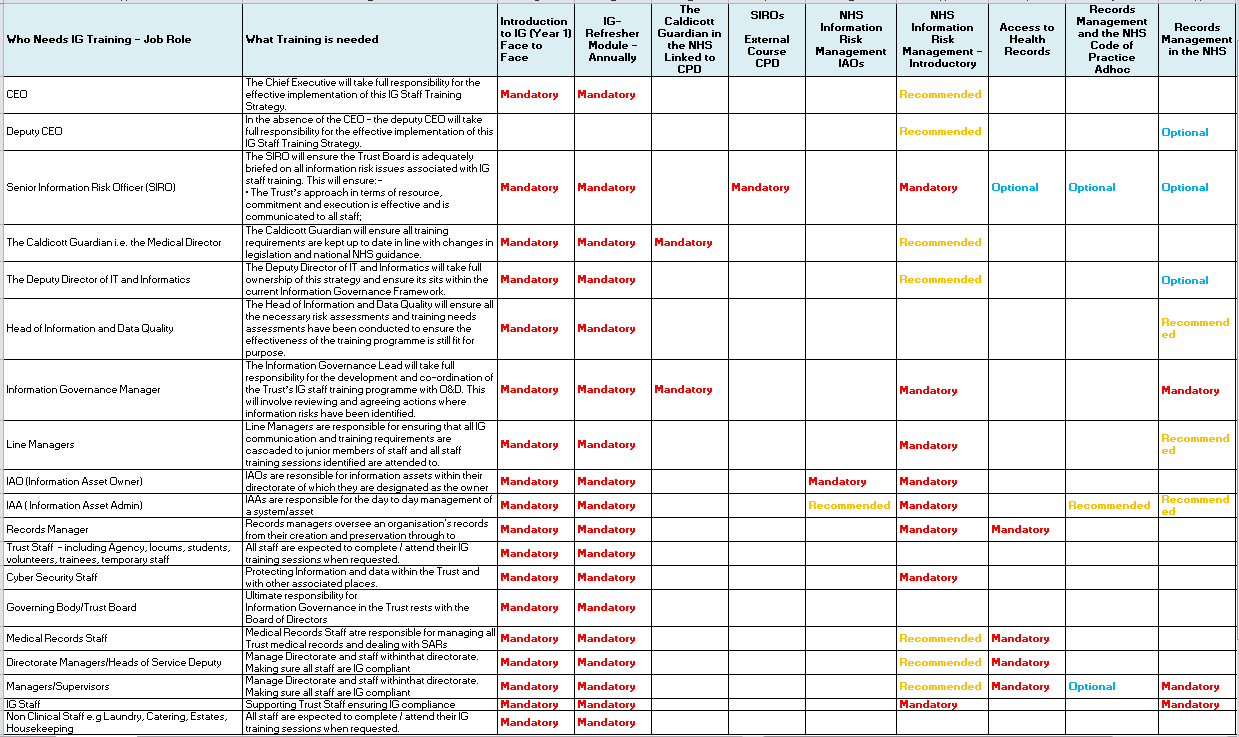
D: Information Governance Standard Operating Procedures Structure

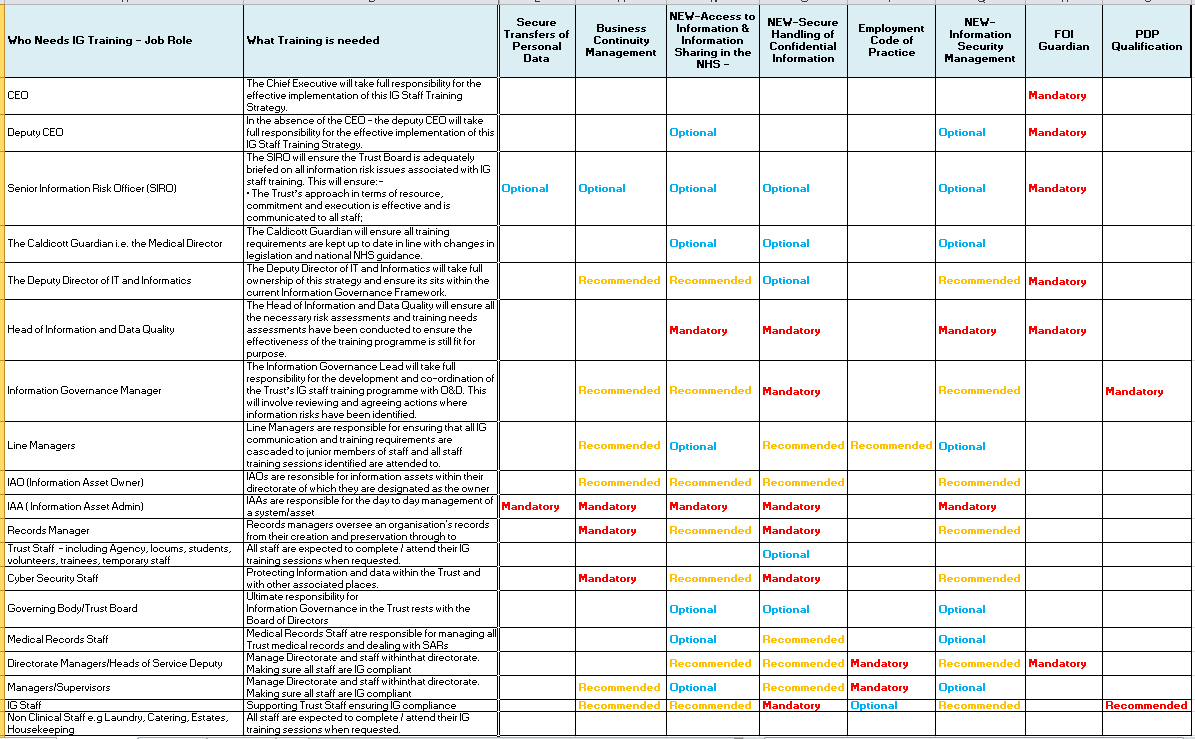
E: Offences relating to personal data

F: Enforcement powers against the organisation

G: Corporate Records Management Committee Guardians

## Appendix C: IG Training Needs Analysis for 2018-2020

contd/



## Appendix D - IG Standard Operating Procedure Structure

|  |  |  |
| --- | --- | --- |
|  | **IG Standard Operating Procedure Structure** | |
| SOP Category | | SOP Name |
| **Access to Information** | | * Access to Personal and Health Information * Staff Access to Own Information * Complaints and/or Concerns to the Data Protection Officer regarding Access to Information * Process for preparing information |
| **Corporate Records** | | * Management of Corporate Records * Retention and Disposal of Corporate Records * Storage and Retrieval of Corporate Records * Transferring Corporate Records to a Local Place of Deposit * Transfer of sensitive Corporate Reports |
| **Healthcare Records** | | * Management of Health Records * Retention and Disposal of Healthcare Records * Storage and Retrieval of Healthcare Records to and from the Medical Records Library * Sharing of patient Healthcare Records to support transfer of patientcare to another hospital. * Transferring Corporate Records to a Local Place of Deposit * Transportation of Healthcare Records off site * Transportation of Healthcare Records on site with the patient * Transportation of Healthcare Records to off-site clinics by Clinicians * Standards for the security of Healthcare Records on the Ward. |
| **Healthcare Records Management** | | * Amendment to Healthcare Records   + Amendment to Healthcare Records or Discharge Summary – Paper   + Amendment to Healthcare Records or Discharge Summary – Electronic * Healthcare Records – Creation, Use and Management * Retention and Disposal of Healthcare Records * Release of Information to Police, Courts and Other Authorities |
| **Access to Healthcare Information** | | * By the patients, representatives, employees and or a member of the public. * On behalf of a patient who lacks capacity (Power of Attorney) * Deceased patients * Release of Information to the Police, Courts and Other Authorities. |
| **Data Protection, Confidentiality and Security** | | * Breach Notification and escalation * Complaints and Concerns * Information Governance Departmental Compliance Audit * Shared emails and calendars |
| **Corporate Records Management** | | * Storage and Retrieval of Electronic Corporate Records * Retention and Disposal of corporate records * Transferring Corporate Records to a local place of deposit ( National Archives) * Corporate and Data Quality * Audits * Email Standards and Procedures * Faxing Standards and Procedures * NHS Mail:   + - * Email, SMS Text Messaging and Faxing Standards and Procedures * Procedures to authorise access a member of staffs emails due to sickness, absence. * Storage of paper corporate records |
| **Freedom of Information** | | * Requests Procedure * FOI Complaints * FOI Internal Reviews and Public Interest * Internal Escalation of Directorate/Departmental none compliance |
| **Information Asset Management/Security** | | * IG Contract Compliance Assessment * Business Continuity * Disaster Recovery * Third Party/Data Processor Assurance Process * Data Flow mapping Procedures * Data Protection Impact Assessments * Audit/Compliance Assessments * Registration Authority Smartcard Management * Care CERT Management: Recording, escalation and reporting * Asset Disposal: Equipment, devices, systems, applications * Asset Decommissioning * Approval of the use of Apps to process or hold personal data * Registering external data bases or websites holding personal information (patient/staff) * Procedure governing the use of mobile devices * Reporting lost or stolen IT equipment * Removable media security standards |
| **Investigations** | | * Forensic Readiness Procedures * Procedure to monitor Trust owned equipment: Email, Internet, social media, system, application and or devices * Reporting of inappropriate usage of the intranet, Trust assets and or devices. |
| **Information Sharing Procedures** | | * 3rd party access to systems and compliance monitoring * Incident reporting and investigations * How to raise data quality concerns * Governance/Liability/Responsibilities * Data Transfers |
| **Information Sharing to Support the Sustainability and Transformation Programme (STP)** | | * Data Privacy Impact Assessments * Data Controller/Data Processor Responsibilities   + Anonymisation and Pseudonymisation Procedures   + Data Transfers   + Data repositories |

## Appendix E - Offences relating to personal data

**Unlawful obtaining etc., of personal data**

1. It is an offence for a person knowingly or recklessly—
2. to obtain or disclose personal data without the consent of the controller,
3. to procure the disclosure of personal data to another person without the consent of the controller, or
4. after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.
5. It is a defence for a person charged with an offence under subsection (1) to prove that the obtaining, disclosing, procuring or retaining—
6. was necessary for the purposes of preventing or detecting crime,
7. was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or
8. in the particular circumstances, was justified as being in the public interest.
9. It is also a defence for a person charged with an offence under subsection (1) to prove that—
10. the person acted in the reasonable belief that the person had a legal right to do the obtaining, disclosing, procuring or retaining,
11. the person acted in the reasonable belief that the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it, or
12. the person acted—
13. for the special purposes,
14. with a view to the publication by a person of any journalistic, academic, artistic or literary material, and
15. in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or retaining was justified as being in the public interest.
16. It is an offence for a person to sell personal data if the person obtained the data in circumstances in which an offence under subsection (1) was committed.
17. It is an offence for a person to offer to sell personal data if the person—
18. has obtained the data in circumstances in which an offence under subsection (1) was committed, or
19. subsequently obtains the data in such circumstances.
20. For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale is an offer to sell the data.
21. In this section—
22. references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 59(8) or 105(3) of this Act (processor to be treated as controller in certain circumstances);
23. where there is more than one controller, such references are references to the consent of one or more of them.

**Re-identification of de-identified personal data**

1. It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.
2. For the purposes of this section and section 172—
3. personal data is “de-identified” if it has been processed in such a manner that it can no longer be attributed, without more, to a specific data subject;
4. a person “re-identifies” information if the person takes steps which result in the information no longer being de-identified within the meaning of paragraph (a).
5. It is a defence for a person charged with an offence under subsection (1) to prove that the re-identification—
6. was necessary for the purposes of preventing or detecting crime,
7. was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or
8. in the particular circumstances, was justified as being in the public interest.
9. It is also a defence for a person charged with an offence under subsection (1) to prove that—

(a) the person acted in the reasonable belief that the person—

1. is the data subject to whom the information relates,
2. had the consent of that data subject, or
3. would have had such consent if the data subject had known about the re-identification and the circumstances of it,

(b) the person acted in the reasonable belief that the person—

1. is the controller responsible for de-identifying the personal data,

(ii) had the consent of that controller, or

1. would have had such consent if that controller had known about the re-identification and the circumstances of it,

(c) the person acted—

1. for the special purposes,
2. with a view to the publication by a person of any journalistic, academic, artistic or literary material, and
3. in the reasonable belief that in the particular circumstances the re-identification was justified as being in the public interest, or
4. the effectiveness testing conditions were met (see section 172).
5. It is an offence for a person knowingly or recklessly to process personal data that is information that has been re-identified where the person does so—
6. without the consent of the controller responsible for de-identifying the personal data, and

(b) in circumstances in which the re-identification was an offence under subsection (1).

1. It is a defence for a person charged with an offence under subsection (5) to prove that the processing—

(a) was necessary for the purposes of preventing or detecting crime,

(b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or

(c) in the particular circumstances, was justified as being in the public interest.

1. It is also a defence for a person charged with an offence under subsection (5) to prove that—

(a) the person acted in the reasonable belief that the processing was lawful,

(b) the person acted in the reasonable belief that the person—

(i) had the consent of the controller responsible for de-identifying the personal data, or

(ii) would have had such consent if that controller had known about the processing and the circumstances of it, or

(c) the person acted—

(i) for the special purposes,

(ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

(iii) in the reasonable belief that in the particular circumstances the processing was justified as being in the public interest.

1. In this section—
   1. references to the consent of a controller do not include the consent of a person who is a controller by virtue of Article 28(10) of the GDPR or section 59(8) or 105(3) of this Act (processor to be treated as controller in certain circumstances);
   2. where there is more than one controller, such references are references to the consent of one or more of them.

**Re-identification: effectiveness testing conditions**

1. For the purposes of section 171, in relation to a person who re-identifies information that is de-identified personal data, ‘the effectiveness testing conditions’ means the conditions in subsections (2) and (3).
2. The first condition is that the person acted—

(a) with a view to testing the effectiveness of the de-identification of personal data,

(b) without intending to cause, or threaten to cause, damage or distress to a person, and

(c) in the reasonable belief that, in the particular circumstances, re-identifying the information was justified as being in the public interest.

1. The second condition is that the person notified the Commissioner or the controller responsible for de-identifying the personal data about the re-identification—

(a) without undue delay, and

(b) where feasible, not later than 72 hours after becoming aware of it.

1. Where there is more than one controller responsible for de-identifying personal data, the requirement in subsection (3) is satisfied if one or more of them is notified.

**Alteration etc., of personal data to prevent disclosure to data subject**

1. Subsection (3) applies where—

(a) a request has been made in exercise of a data subject access right, and

(b) the person making the request would have been entitled to receive information in response to that request.

1. In this section, “data subject access right” means a right under—

(a) Article 15 of the GDPR (right of access by the data subject);

(b) Article 20 of the GDPR (right to data portability);

(c) section 45 of this Act (law enforcement processing: right of access by the data subject);

(d) section 94 of this Act (intelligence services processing: right of access by the data subject).

1. It is an offence for a person listed in subsection (4) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.
2. Those persons are—

(a) the controller, and

(b) a person who is employed by the controller, an officer of the controller or subject to the direction of the controller.

1. It is a defence for a person charged with an offence under subsection (3) to prove that—

(a) the alteration, defacing, blocking, erasure, destruction or concealment of the information would have occurred in the absence of a request made in exercise of a data subject access right, or

(b) the person acted in the reasonable belief that the person making the request was not entitled to receive the information in response to the request.

**Offences under the Computer Misuse Act 1990**

The Act introduced three criminal offences:

* Unauthorised access to computer material.
* Unauthorised access with intent to commit or facilitate commission of further offences.
* Unauthorised modification of computer material.

The maximum penalty is 10 years ’**imprisonment’** and a fine. The Computer Misuse Act has also been changed to make it an offence to make, adapt, supply or offer to supply any article which is ‘likely to be used to commit, or to assist in the commission of, [a hacking or unauthorised modification] offence’.

**Freedom of Information Act 2000**

You may be breaching the Freedom of Information Act if you do any of the following:

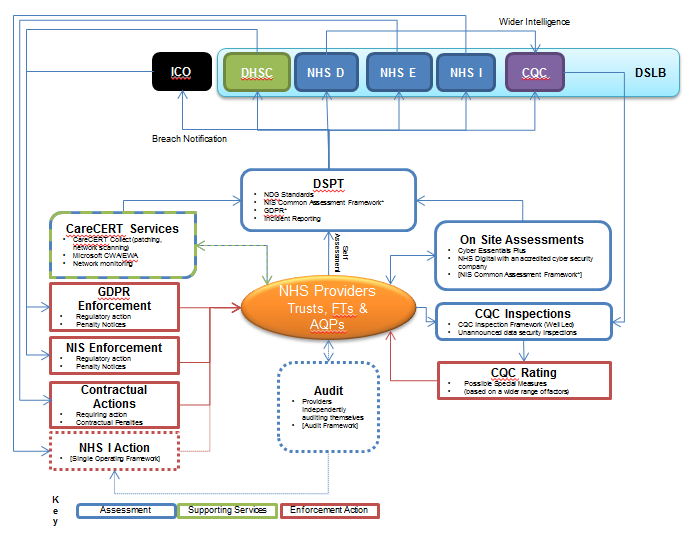
* fail to respond adequately to a request for information;
* fail to adopt the model publication scheme, or do not publish the correct information; or
* deliberately destroy, hide or alter requested information to prevent it being released.

*This last point is the only criminal offence in the Act that individuals and public authorities can be charged with.*

Other breaches of the Act are unlawful but not criminal.

## Appendix F - External Governance, oversight, enforcement and reporting arrangements within the NHS

**NHS X**





NHS England leads the National Health Service (NHS) in England. They set the priorities and direction of the NHS and encourage and inform the national debate to improve health and care. To give everyone greater control of their health and their wellbeing, and to be supported to live longer, healthier lives by high quality health and care services that are compassionate, inclusive and constantly-improving.



The National Data Guardian (NDG) advises and challenges the health and care system to help ensure that citizens’ confidential information is safeguarded securely and used properly.



The Department of Health & Social Care supports ministers in leading the nation’s health and social care to help people live more independent, healthier lives for longer.

**Data Security Leadership Board (DSLB)**

The Department of Health and Social Care’s (DHSC) Data Security Leadership Board (DSLB) was commissioned the Chief Information Officer (CIO) for the health and social care system in England to carry out a review of May 2017’s WannaCry cyberattack. The objectives of the review were to:

* Analyse key lessons learned from the WannaCry cyber-attack;
* Assess actions required to mitigate the risk and impact of a future cyberattack looking in particular at infrastructure, incident response and resilience; and
* Ensure this learning is shared widely across the health and care system.



NHS Improvement, the financial regulator of NHS Trusts in England. NHS Improvement supports NHS Trusts to ensure patients receive consistently safe, high quality, compassionate care within local health systems that are financially sustainable.

NHS Improvement has the following enforcement powers under legislation:

* Informal action;
* Enforcement undertakings;
* Discretionary requirements;
* Section new licence conditions (and or revoke a licence to provide services);
* Remove, suspend or disqualify directors or governors;
* Provides concurrent powers with the Office of Fair Trading in connection with the Completions Laws.

The discretionary requirements NHS Improvement can impose are:

* compliance requirements which require a provider to take such steps as we may specify to ensure that the breach in question does not continue or recur;
* restoration requirements which require a provider to take such actions as we may specify to restore the situation to what it would have been, absent the breach; and
* variable monetary penalties which require a provider to pay a penalty.

Additional information about the NHS Improvement can be found on their website: <https://improvement.nhs.uk>



NHSX brings teams from the Department of Health and Social Care, NHS England and NHS Improvement together into one unit to drive digital transformation and lead policy, implementation and change.

They are a diverse team with a range of skills and expertise, including clinicians, technologists, policy experts, developers, data scientists and project managers.

They report directly to the Secretary of State and the Chief Executive of NHS England and NHS Improvement.

<https://www.nhsx.nhs.uk/>



The CQC are the independent regulator of health and adult social care in England. They are there to ensure health and social care services provide people with safe, effective, compassionate, high-quality care and we encourage care services to improve.

The Health and Social Care Act 2012 gave CQC new legal responsibilities from 1 April 2013 to monitor and seek to improve the information governance practices of registered providers.

CQC has the following enforcement powers under legislation:

The CQC may if appropriate issue warning notice under Section 29A of the Health and Social Care Act 2008 when they believe that the quality of healthcare at an NHS trust or foundation trust requires significant improvement.

Additional information about the CQC can be found on their website: <https://www.cqc.org.uk/>



NHS Digital (NHSD) is an executive non-departmental public body, accountable to the Secretary of State for Health and to Parliament.

NHS Digital's statutory role is set out in the Health and Social Care Act 2012, and additional requirements are conferred on the organisation through the Care Act 2014. NHS Digital may also undertake additional functions under directions from the Department of Health (DH) or the NHS Commissioning Board (publicly known as NHS England.

The operational relationship between DH and NHSD is set out in the Framework Agreement signed by both parties. The agreement requires organisations providing NHS services to annually successfully complete the Data Security and Protection Toolkit. This is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian’s 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

Under the terms of the NHS contract to provide clinical services all providers are required to collaborate with NHS Digital in the procurement and implementation of HSCN, the replacement for N3: <http://systems.digital.nhs.uk/hscn>

Providers are also required to successfully complete the NHS Digital Data Security and Protection Toolkit (DSPT) annually.

Additional information about NHS Digital can be found on their website: <https://digital.nhs.uk>

 [www.ico.org.uk](http://www.ico.org.uk)

**Information Commissioner’s Office Powers**



Under GDPR, DPA 2018 and eIDAS, the ICO have the authority to issue enforcement notices, assessment notice (for a compulsory audit) or information notice (requiring you to provide us with information for our investigation) we also have the power to impose more substantial fines of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.



The FOIA 2000, and ER legislations provide the ICO with the following tools at their disposal if a public authority repeatedly or seriously fail to meet the requirements of the legislation, or conform to the associated codes of practice, the ICO can take the following action:

* conduct an organisational audit
* serve information notices requesting actions to be taken
* serve an enforcement notice
* issue recommendations specifying steps the organisation should take to comply;
* issue decision notices detailing the outcome of the ICO’s investigation to publically highlight particular issues with an organisation’s handling of a specific request;
* prosecute those who commit criminal offences under the Act; and
* report to Parliament on Freedom of Information issues of concern.



NIS is derived from a European law (the ‘NIS Directive’) and is intended to establish a common level of security for network and information systems. NIS aims to address the threats posed to them from a range of areas, most notably cyber-attacks. NIS concerns the security of ‘network and information systems’. NIS requires these systems to have sufficient security to prevent any action that compromises either the data they store or any related services they provide.

The ICO has a range of enforcement powers that they can use, where appropriate:

* they can issue information notices that require you to provide us with certain information;
* they can issue enforcement notices that require you to take, or refrain from taking, particular steps or actions;
* they can issue monetary penalties for material contraventions, up to a maximum of £17 million in the most serious cases; and
* they also have powers of inspection



The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

* marketing calls, emails, texts and faxes;
* cookies (and similar technologies);
* keeping communications services secure; and
* customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

The ICO has several ways of taking action to change the behaviour of anyone who breaches PECR. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner can also serve a monetary penalty notice imposing a fine of up 4% of Global turnover or 20 million Euro’s whichever is the greater.

## Appendix G - Corporate Records Management Committee Guardians



**INFORMATION REGARDING GUARDIANS FOR THE**

**CORPORATE RECORDS MANAGEMENT COMMITTEE**

**Overview**

In today's world, accurate and accessible corporate record-keeping is vitally important for good governance and compliance. This imperative has elevated the practice of entity management to a position of exceptional importance for governance and compliance professionals.

The Information Guardian will work in their own area and wider across the Trust to promote awareness and engagement with the Trust’s quality goals, ensuring the development of a culture of care, teamwork, improvement and innovation in accordance with the organisations values.

When working to encourage adoption, the guardian plays an integral part in this process by working to achieve greater buy-in and collaboration.

The role is voluntary, but time away from the current role (approx. 2 hours per month) will be given to undertake the role. Attendance to the CRMC may be required if the committee member you work with is unable to attend (the CRMC meets once a month).

**Role to play**

This is a new initiative and it is likely that the role will develop as the project itself does. The following tasks are currently envisaged:

The simplest way to define an "Information Guardian" is this—someone who recognizes the need for improvement or flaws in current entity management processes, and who will facilitate the introduction of a new, streamlined and more effective solutions.

The Guardian will communicate how the new solution works and the specific benefits it confers in each department. Ensuring that communications from the CRMC to the workforce is appropriate and effective and that messages are being delivered to all staff in a timely and consistent manner.

Once the adoption phase is complete and the solution is running seamlessly, the guardian still has a key role to play—ensuring that everything remains current. This means monitoring and staying abreast of trends to determine whether the existing information has evolved with the times. So continue to work with colleagues to embed a ‘culture of quality’ across their department and sometimes wider area, reminding users of the inherent risks of having older data (spreadsheets, for example) in circulation.

To liaise with other information guardians for purposes of promoting the CRMC agenda in a consistent and coordinated manner and to raise concerns through the appropriate routes in relation to activities which are impacting on the delivery of quality services and to signpost colleagues to appropriate processes for raising concerns.

**Qualities of a Guardian**

Guardians should be able to demonstrate passion and commitment to improving quality of accuracy and accessibility corporate record in their own role.

Possess the ability to see solutions instead of barriers with a ‘can do’ attitude.

Enthusiasm and ability to motivate and inspire others through a positive approach to providing high quality services through excellent communication skills

Have the confidence to challenge practice which does not appear to contribute to the organisations quality goals and excellent corporate record-keeping.

**Benefits**

While helping organizations run more effectively and staying on the right side of compliance are the primary benefits, there are also personal rewards that the champion reaps.

Company recognition, for example, may be forthcoming after the solution is successfully implemented. The guardian also becomes recognized as a leader and authority in this realm, a go-to person for essential support and guidance.

Filling the guardian's role also exhibits strong leadership, which can play a key part in someone's professional development or career progression.

Playing a critical lead role in the transformation of corporate record management is not an accolade that just anyone can claim. It indicates that the guardian is a forward-thinking and resourceful leader with the technical know-how to implement core internal processes.

**Challenges**

In order to be successful, it's imperative to not only generate organizational support but to also secure the necessary resources to guarantee the project is viable. Prospective guardians should also consider the risks inherent in changing a longstanding practice, process or workflow. Even if the solution is innovative and rewarding, users must depart from their comfortable routines in order to adapt to something new. The guardian must provide reassurance that these risks are worth taking, in an effort to achieve more efficient and effective outcomes through digital transformation.

Coordination is another key challenge. In order for this transition to work, organizational buy-in must be accompanied by inter-departmental collaboration. Guardians must also be comfortable taking a leading role, as all eyes will be firmly affixed on them as they coordinate the transition but always fully supported by the Corporate Records Management Committee.