Information Governance Policy and Strategic Management Framework

Including the Information Governance Strategy

Document No.	WHCS 05	Version No.	1.0
Approved by	**Policies and Procedures Group**	Date approved	Via e.mail voting March 2019
Ratified by	**Information Governance Policy and Oversight Group**	Date ratified	05/03/2019
Date Implemented		Next Review Date	05/03/2022
Status:		Ratified	
Target Audience		This policy applies to all employees of Wiltshire Health and Care, whether permanent, part-time or temporary (including fixed-term contract). It applies equally to all other staff working for Wiltshire Health Care including private-sector, voluntary-sector, agency, locum, and contract, seconded and volunteer staff that have access to Wiltshire Health Care's ICT systems. For simplicity, they are referred to as 'employees' throughout this policy.	
Accountable Director		Managing Director, Wiltshire Health and Care	
Policy Author/Originator		Information Governance Officer, Salisbury NHS Foundation Trust	
Implementation Lead		Director of Governance and Company Secretary, Wiltshire Health and Care	
If developed in partnership with another agency, ratification details of the relevant agency		Salisbury NHS Foundation Trust, as provider of Wiltshire Health and Care's Information Governance service.	

Version No.	Updated By	Updated On	Description of Changes
0.1	Katherine Hamilton Jennings, Director of	30 January 2019	Adaptions to support the policy's implementation

	Governance and Company Secretary June Foster, Business Manager		within Wiltshire Health and Care. Layout and format is in line with WHC's guidelines.

Contents

Glossary

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

1. Policy Statement, Aims & Objectives

Wiltshire Health and Care 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.

1.1 This document sets out Wiltshire Health and Care's policy for Information Governance within the organisation. This policy includes the Information Governance Framework and all associated procedures.

1.2 Wiltshire Health and Care 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 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.

1.3 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.

1.4 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

1.5 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:

- Wiltshire Health and Care 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 Wiltshire Health and Care.
- 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.

1.6 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 Learning and Development team on Information Governance/Security Training Policy Compliance Reports
3	Production of quarterly Standard Assurance reports to the Information Governance Policy and Oversight Group (IGPOG)	Reporting
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

2. 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
- 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)

3. 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.

4. Responsibilities and Accountability

4.1 Overall accountability for ensuring that there are systems and processes to effectively manage information governance lies with the Managing Director.

It is the responsibility of all managers 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
Director of Quality, Professions, and Workforce	**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 Governance and Company Secretary	**Senior Information Risk Owner**	Has delegated responsibility for: • Overseeing the development and maintenance of relevant information governance policies and procedures. Via the Information Governance Policy and Oversight 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** which defines in detail the SIRO's Accountability and Organisational Accountability Framework.
IG/ RA Manager (Salisbury NHS Foundation Trust)	**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. • Providing advice in relation to, and ensuring the correct management of, FOIA requests made to Wiltshire Health and Care. • Overseeing Information Governance training compliance. • Contributing to governance-related audits and working with Internal Audit to assess progress, developing action plans as required. • Providing advice in relation to the conduct

		of information governance related incidents, ensuring the development of action plans and external reporting where appropriate. • Ensuring that there is appropriate liaison with other committees and groups within the organisation to promote and integrate information governance. • Advising on the appropriate management of clinical and corporate records. 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, support in the completion of these assessments, advise on when it is appropriate for these to be signed-off, and advise on how the information within the assessments is communicated externally • 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 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.
Managers	**Information Asset Owners**	Information Asset Owners are responsible for providing regular reports to the Senior Information Risk Owner (SIRO), 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 the Information Governance team at SFT. • 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. **Please refer to section 9.2** for details the role of IAO reporting structure within Wiltshire Health and Care.
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** compliance with 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 to maintain relevant parts of the 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 Wiltshire Health & Care'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 IAA reporting structure within Wiltshire Health & Care
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.

4.2 The Information Governance Policy and Oversight Group (IGPOG) has delegated responsibility for overseeing information governance management from the Executive Committee. It will monitor compliance with Information Governance requirements through standing reports and management activities:

4.2.1 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 (managed by GWH)
- Subject Access Request

4.2.2 Annual Audit:

- Clinical Records Audit
- Confidentiality and Protection Audit
- Cyber Essentials Audit
- Data Security and Protection Audit
- Informatics Penetration Audit

These audits will be facilitated by/conducted by the SFT Information Governance team.

4.2.3 Management Activities

They 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 on 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 Wiltshire Health and Care Board (via the Executive Committee), 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.

4.2.4 Review

This document will 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

They will also ensure that this Information Governance Policy and Strategic Management Framework will act as an overarching framework for the local delivery of Information Governance.

4.2.5 Monitoring

This policy will be performance monitored to ensure that it is in-date and relevant to the core business of Wiltshire Health and Care. The results will be published in the regular highlight report to the Executive Committee.

4.3 The Information Governance Policy and Oversight Group's (IGPOG) purpose is to:

- Guide Wiltshire Health and Care 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 Wiltshire Health and Care'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 Data Security and Protection Toolkit and General Data Protection Regulations (GDPR) or equivalent each year;
- Approve any action plans stemming from the IG work plan and monitor their implementation;
- Review and maintain the Information Governance Strategy, and all related policies / procedures on behalf of Wiltshire Health and Care (notwithstanding that advice on the content of the same will come from the Information Governance team at SFT);
- Review any risks or incidents in relation to Information Governance and ensure that appropriate actions have been taken and escalation processes are implemented and monitored for IG incidents;

- Ensure that Wiltshire Health and Care's approach to information handling is communicated to all staff and made available to the public (where applicable) by reviewing, amongst other things, training programmes, fair processing notices/ privacy notices, and communication plans;
- Review the results of any Information Governance audits and oversee the implementation of any remedial actions;
- Ensure that the SIRO and Caldicott Guardian are appropriately briefed on the activities of the IGPOG;
- 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 Policy and Oversight Group shall take place on at least a quarterly basis with a key membership including the SIRO, Caldicott Guardian, DPO, Head of Information Communication Technology, Corporate Services Business Manager, Director of Finance, Contracts Manager, as well as the Cyber Security Specialist (or an individual acting on their behalf). 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 Wiltshire Health & Care. The group's terms of reference are refreshed on an annual basis to develop a work plan to deliver the above duties.

5. Training

All staff are required to complete basic information governance and data protection training annually, and will also be asked to complete other training commensurate with their duties and responsibilities. Appendix C provides details of Wiltshire Health and Care's training needs analysis conducted by the IG department (Salisbury NHS Foundation Trust) 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 (CBTs)
- 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 Information Governance Team at Salisbury NHS Foundation Trust if there are specific training needs.

Section B – IG Policy and Strategic Management Framework

1. Introduction

This section sets out the approach to be taken within Wiltshire Health and Care to provide a robust Information Governance framework for the management of information. It addresses key areas for Information Governance development across Wiltshire Health and Care 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 T-Drive to improve staff awareness of Wiltshire Health and Care's approach to future Information Governance developments.

1.1. 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, 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 Directorate/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

- **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 T-Drive to access the most up to date guidance and documents.

1.2 The Information Governance Policy and oversight Group (IGPOG) oversees the Information Governance agenda.

1.3 The following organisational resources are available to support the IGPOG:

- IG/RA Manager/Data Protection/Privacy Officer, Salisbury NHS Foundation Trust
- Information Governance team, Salisbury NHS Foundation Trust
- Managing Director, Wiltshire Health and Care
- Director of Governance and Company Secretary, Wiltshire Health and Care
- Director of Quality, Professions, and Workforce, Wiltshire Health and Care
- Director of Finance, Wiltshire Health and Care
- Director of Infrastructure, Wiltshire Health and Care
- Contracts Manager, Wiltshire Health and Care
- Head of People, Wiltshire Health and Care
- Head of Information Communication Technology, Wiltshire Health and Care
- Cyber Security Specialist (within GWH)
- Information Asset Owners
- Information Asset Administrators

2. Strategic Aims

Wiltshire Health & Care 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 staff through an e-learning programme. Wiltshire Health and Care'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 Wiltshire Health and Care	Incident Reporting Staff Survey Complaints Compliments Training Compliance Reports

Openness & Transparency	Openness and transparency will be promoted via Wiltshire Health and Care'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 are examples of how Wiltshire Health and Care 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: • **Staff training and awareness -** successful completion of the NHS Digital IG training by employees; staff awareness campaigns, articles and newsletter articles.	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.

	Wiltshire Health and Care 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 location on the Wiltshire Health and Care website, displaying the privacy notice describing how Wiltshire Health and Care holds their data. All employees are made aware of the privacy notice setting out how Wiltshire Health and Care holds their data, 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.		

Aim	Detail	Outcome	Measures
Data Security and Protection Toolkit Compliance	Wiltshire Health and Care 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.	Wiltshire Health and Care 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 through Wiltshire Health and Care's Incident Management System. 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,	Improved incident reporting and hence, better understanding of real and potential risks requiring action.	Compliance Reports

	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.		
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	Wiltshire Health and Care will ensure that the data it uses is as accurate and up-to-date as possible. Wiltshire Health and Care 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. Wiltshire Health and Care supports data quality	Clear procedures around validation checks carried out and improved accuracy of information.	Audit Compliance Reports Spot checks

	across its services to ensure the provision of accurate data to support management and the procurement of patient services. Wiltshire Health and Care ensures robust data quality checks are built in to the introduction and ongoing development of technological solutions to improve and manage records.		
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 Health 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. Wiltshire Health and Care 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 organisation 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	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

	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 Wiltshire Health and Care 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.		
Aim	**Detail**	**Outcome**	**Measures**
Records Storage and Maintenance (Records Management / Information Lifecycle Strategic Aims)	All manual and electronic records owned by Wiltshire Health and Care will be appropriately stored and maintained in accordance with guidance and legislation (see Records Management Procedure). **Manual Records:** Storage facilities for current paper records require 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	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

	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 T-drive.		

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 IG assurance 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 the Information Governance team and Salisbury NHS Foundation Trust, if required. Methods of disposal of records must meet confidentiality and security guidelines. For records		Audit Reports and Destruction Logs submitted by departments

	disposed of by a contractor, the contractor will be required to sign confidentiality agreements and produce written certification as proof of destruction. Action to 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.		
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	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.

	procedures (Policy on Procedural Documents). Other guidance will be available on the T-Drive or from the Corporate Services team.		

3. Openness, Transparency and Information Sharing

3.1 Wiltshire Health and Care will ensure that the principles of Caldicott and the regulations outlined in the General Data Protection Regulation and Wiltshire Health and Care's Information Governance Procedure underpin the management of confidential information at all times.

3.2 Wiltshire Health and Care 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.

Wiltshire Health and Care 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 Wiltshire Health and Care newsletter, staff emails, the intranet, promotional materials, training packages, and meetings.

3.3 As a Data Controller organisation, Wiltshire Health and Care are 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 Wiltshire Health and Care's Notification, the Data Protection Officer will review the types of processing being carried out within Wiltshire Health and Care (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). Wiltshire Health & Care's ICO Registration Number is **ZA190147**.

3.4 Wiltshire Health & Care 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

3.5 Information Sharing and Collaborative Working

Wiltshire Health and Care recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. 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 Procedures (see section 1.1).

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 our Information Sharing Procedures (section 1.1) which define:

- the processes for sharing information with third parties;
- how the organisation can manage the way third parties handle personal and confidential information;
- how information governance fits within supplier relationships and contractual obligations;
- measurements and metrics for third parties meeting Wiltshire Health and Care's information governance goals.

3.6 Non-confidential information about Wiltshire Health and Care 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.

3.7 Patients have free access to their own healthcare information. Wiltshire Health and Care 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.

4. Information Security

4.1 Information security risk is inherent in all administrative and business activities and everyone working for, or on behalf of, Wiltshire Health & Care 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.

4.2 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

4.3 Wiltshire Health and Care 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.

4.4 Wiltshire Health & Care will continue to promote effective confidentiality and security practices to its staff through policies, procedures and incorporate it into the IG Training Needs Analysis (see Appendix C).

4.5 Wiltshire Health and Care 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 Wiltshire Health and Care, and recommendations and actions agreed will be performance managed by the Information Governance Policy and Oversight Group.

4.6 Information Asset Owners will liaise with the Information Governance department at Salisbury NHS Foundation trust, who will collate, on behalf of the SIRO, issues relating to information security risks within their area of responsibility.

4.7 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, Wiltshire Health and Care. It must be signed by all contractors prior to entering Wiltshire Health and Care site. This is the responsibility of leads managing those contractors, whether they are management, associates, or facilities contractors.

4.8 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: Information.Governance@salisbury.nhs.uk

4.9 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 Wiltshire Health and Care 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 Wiltshire Health and Care'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.

5. Information Quality Assurance/Data Quality

5.1 Wiltshire Health and Care is in the process of reviewing and establishing procedures to support the information quality assurance and the effective management of records. These will be called the Data Quality Procedure and Records Management Procedure.

5.2 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 Information Governance Policy and Oversight Group.

5.3 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.

6. Data Protection

6.1 Wiltshire Health and Care 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.

Wiltshire Health and Care 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		Expectation
1	**Information is used for limited, specifically stated purposes**	Wiltshire Health & Care 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	**Using the minimum**	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible

	amount necessary	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	**Information is accurate**	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4	**Information is kept in an identifiable format no longer than necessary**	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	**Information is Secure**	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 processed lawfully, fairly and in a transparent manner in relation to individuals**	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.

6.2 Individuals' 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.

6.3 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 Wiltshire Health and Care 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	Wiltshire Health & Care 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 minimum amount 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.

6.4 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.

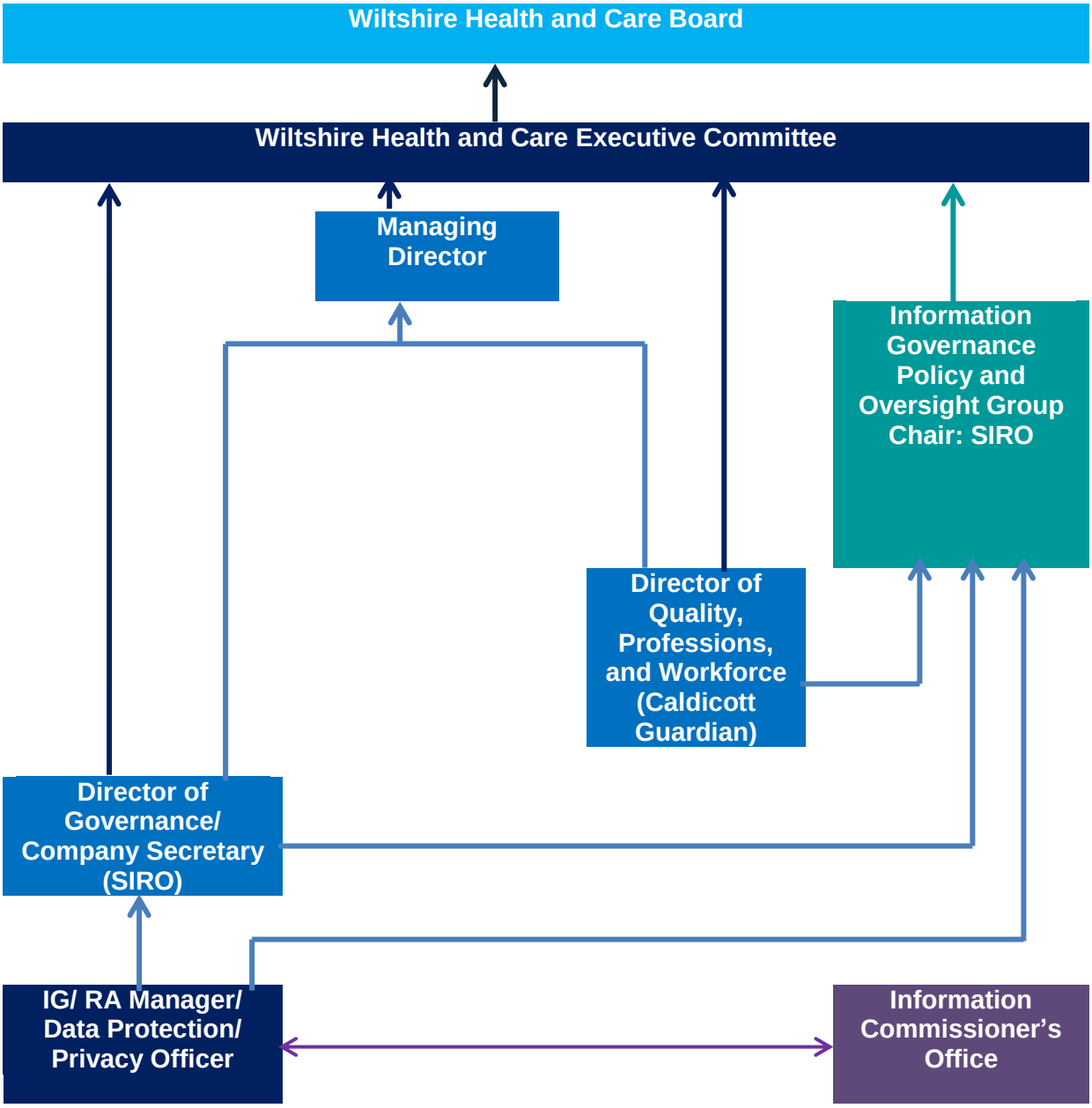
6.4.1 Tasks of a Data Protection Officer

The data protection officer role within Wiltshire Health and Care 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 the GDPR and all other applicable data protection provisions;
- to monitor compliance with the GDPR and all other applicable 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 (ICO);
- 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 Managing Director with Freedom of Information (FOI) request compliance.

6.4.2 Data Protection Officer/IG Manager's Accountability Framework

Diagram 1 - Data Protection Officer/IG Manager's Accountability Framework below illustrates the internal multifunctional reporting, escalation and accountability framework for data protection within Wiltshire Health and Care.



7. Confidentiality

7.1 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.

7.2 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 Caldicott 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 Caldicott Guardian must ensure that they themselves play a key role in actively promoting plans to enable this work to be done. The Caldicott 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.

Wiltshire Health and Care's Director of Quality, Professions, and Workforce is Wiltshire Health and Care's designated Caldicott Guardian.

It is their duty to oversee the Caldicott function.

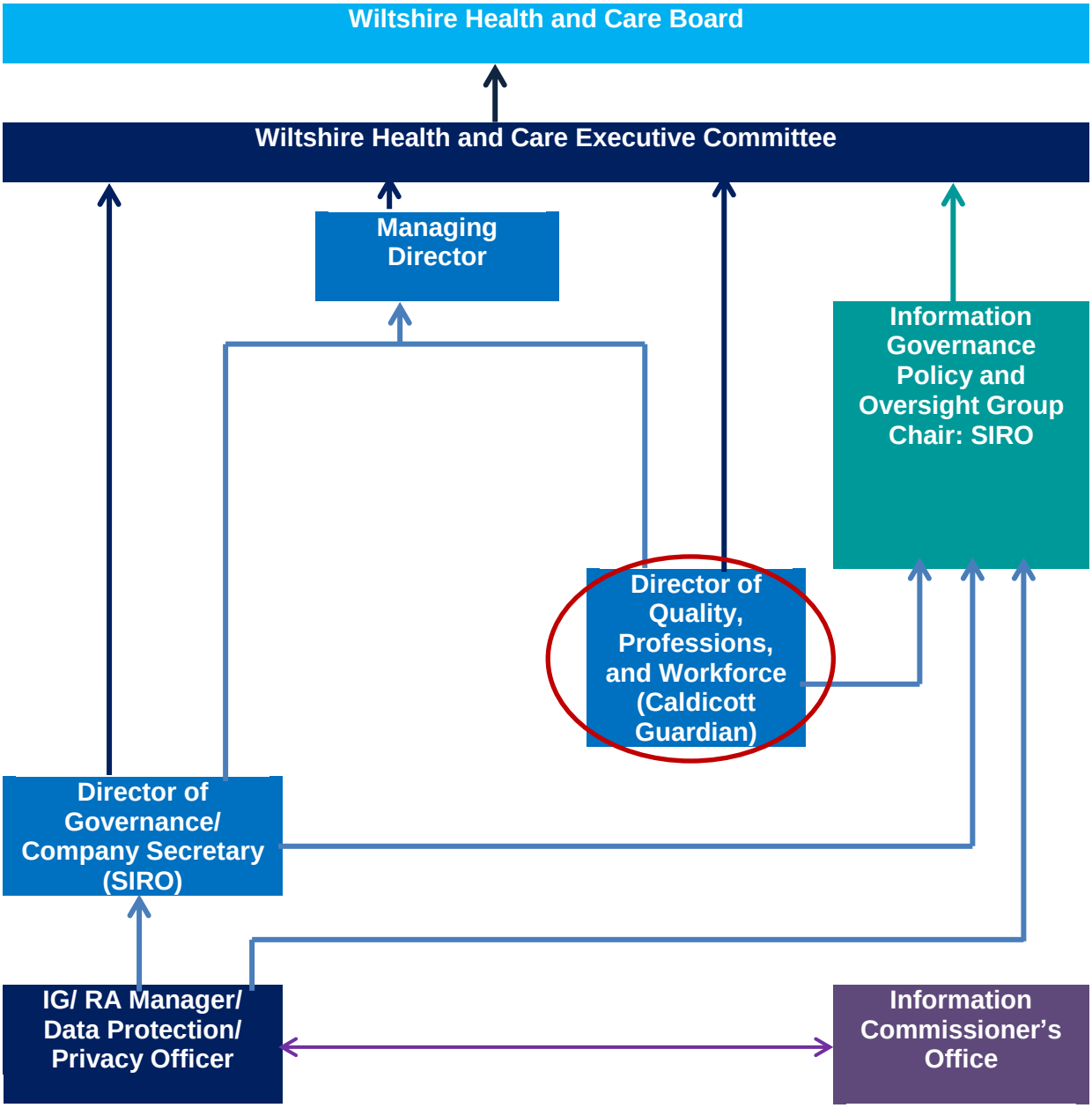
This role's primary concern is upholding and supporting patient confidentiality and ensuring healthcare data is shared appropriately and legally to support patient care pathways across the organisation.

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.

7.3 The Caldicott Guardian Accountability and Organisational Framework

Diagram 2 - Caldicott Guardian Accountability and Organisational Framework below illustrates the internal multifunctional Caldicott reporting, escalation and accountability framework within Wiltshire Health & Care.



7.4 The Seven Caldicott Principles

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

Table 5: 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.

8. Information Risk Management Framework

Information Risk is inherent in Wiltshire Health and Care'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.

Wiltshire Health and Care maintains a Board 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 Framework and Strategy. Information Governance risks are routinely reviewed on behalf of Wiltshire Health and Care's Board by the Information Governance Policy and Oversight Group, and escalated via Wiltshire Health and Care's Senior Information Risk Owner (SIRO).

8.1 Senior Information Risk Owner (SIRO) Responsibilities

The Senior Information Risk Owner (SIRO) acts as an advocate for information risk on the Board. The role of SIRO has been incorporated into the role of the Director of Governance and Company Secretary, whose primary role is to strengthen information security assurance controls and functions within Wiltshire Health and Care, and to provide Wiltshire Health and Care's Board with an annual assurance assessment of security risks (guided by the advice of the Data Protection Officer).

The SIRO is responsible for leading and fostering a culture that values, protects and uses information for the success of the organisation 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:

- Wiltshire Health and Care has a plan to achieve and monitor the right culture, across the organisation 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.

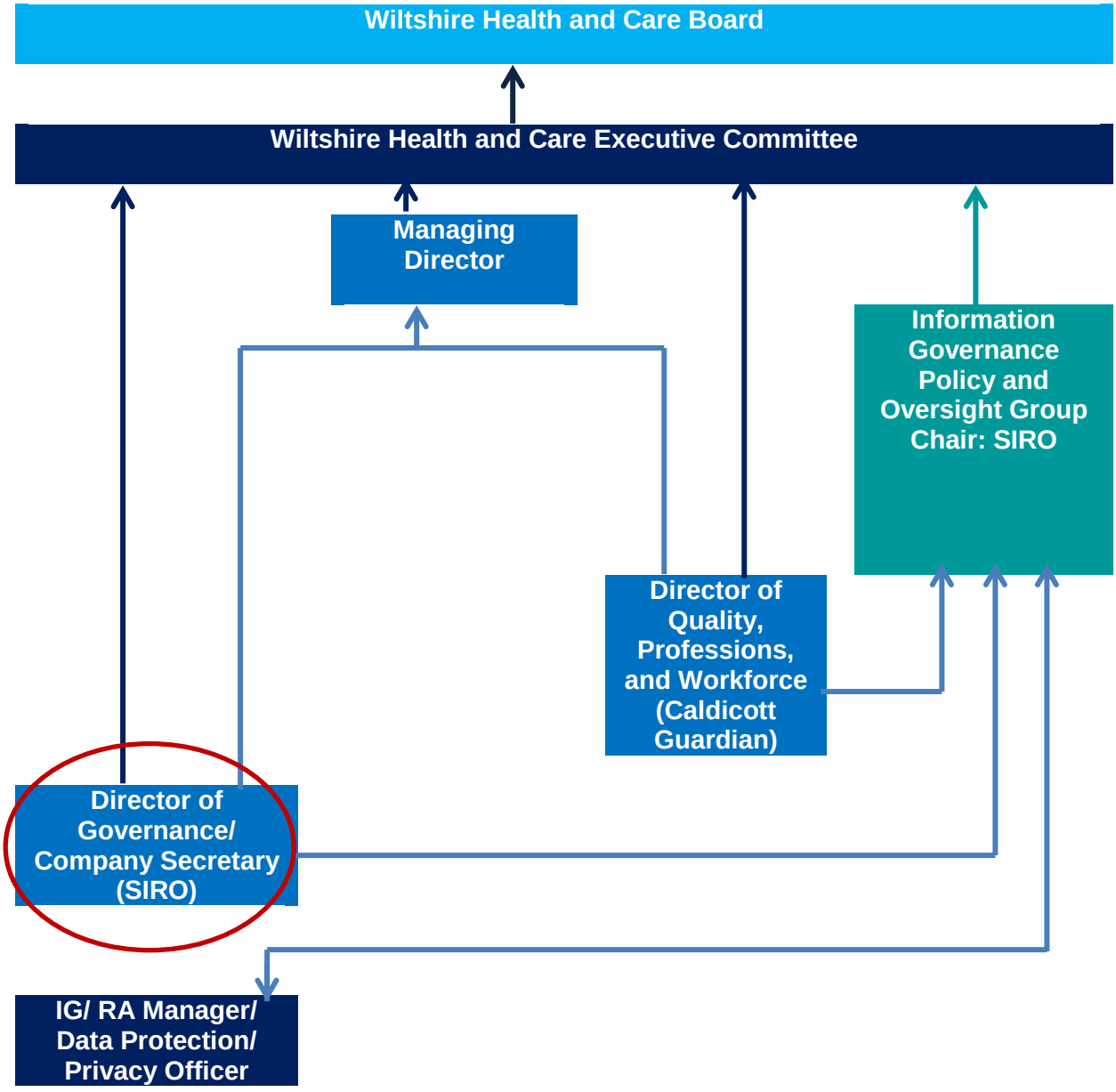
A SIRO must attend and successfully complete an accredited training course endorsed by NHS Digital and NHS England and thereafter complete and pass the relevant NHS Digital e-learning package successfully on an annual basis.

The SIRO is advisor to the Managing Director and Wiltshire Health and Care Board on information security and risk management strategies and provides periodic reports and briefings on progress. Within Wiltshire Health and care, because we are outsourcing specialist Information Governance expertise, these reports are drafted by the Information Governance team at Salisbury NHS Foundation Trust, informed by the risk profile of Wiltshire Health and Care. The SIRO then approves the content, and is responsible for briefing the Managing Director and Board.

8.2 Senior Information Risk Owner Accountability Framework

The Managing Director 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 3 - Senior Information Risk Owner Accountability Framework illustrates the accountability and communication framework between the Managing Director, SIRO, and the Data Protection Officer, providing assurance and escalation compliance relating to information and security risk management and organisational oversight.



The members of the Executive Committee identify and collectively manage risks on behalf of the Board. Directors manage information risks within their portfolios, supported by the designated Information Asset Owners and Information Asset Administrators.

Wiltshire Health and Care's Board and Information Governance Policy and Oversight Group receive an annual report on information governance compliance at three key stages within the financial year.

8.3 Information Risk Management Strategy

It is the objective of Wiltshire Health and Care to ensure information risk management is integrated into Wiltshire Health and Care'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 Information Governance Policy and Oversight Group members.

8.4 Managing Information Security Risks

Wiltshire Health and Care faces many types of risk - internal, external, strategic and those arising from projects or major Government initiatives. The Information Governance policy and Oversight Group proactively monitors information risk by 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 Wiltshire Health and Care's Director of Governance and Company Secretary/Senior Information Risk Owner on behalf of the Board who is collectively accountable for information risk management and has a collective responsibility to ensure that Board provides, reviews, challenges and supports the management of risks.

8.4.1 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 Wiltshire Health and Care and or its systems;
- Before enhancements, upgrades, and conversions associated with critical systems or applications;
- When NHS policy or legislation requires risk determination;
- When Wiltshire Health and Care's Executive management team requires it.

8.5 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.

8.5.1 Information Governance Incident Management

All Information Governance incidents will be formally logged, categorised by severity and analysed in accordance with the Wiltshire Health and Care'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
- Senior Information Risk Owner
- Data Protection Officer

8.5.2 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) Wiltshire Health and Care is legally required to send notification to the ICO via the Data Security and Protection Toolkit within 72 hours.

8.5.3 Learning from Incidents

Learning from risks, incidents and other such events is vital when developing a culture in Wiltshire Health and Care that welcomes the opportunity to improve patient care, and the security and confidentiality of personal information offered by Wiltshire Health & Care 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 Policy and Oversight 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.

9. 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.

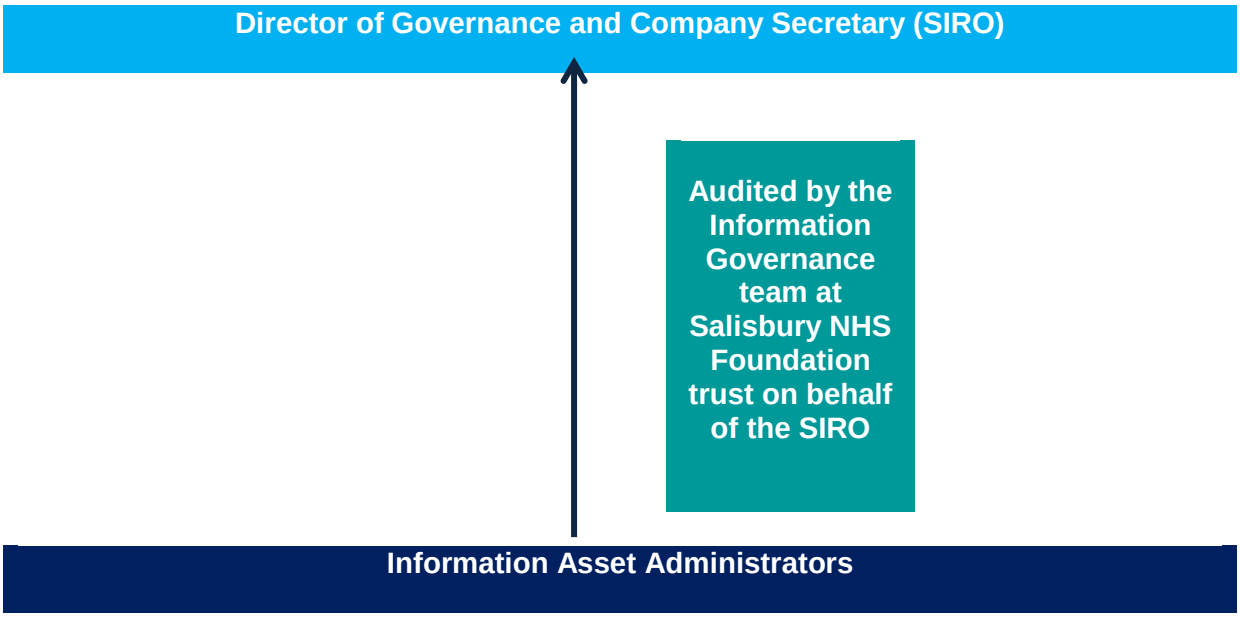
Non-computerised systems holding information must be asset registered with relevant file identifications and storage locations.

Table 6: 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 Wiltshire Health & Care.

9.1 Information Asset Risk Management Assurance Framework

Diagram 4 - internal information risk management reporting accountability framework



9.2 Information Asset Owners

Certain members of the Executive Team at Wiltshire Health and Care are its 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 Wiltshire Health & Care 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.

9.2.1 IAO Responsibilities

- Maintenance of an up-to-date and accurate System Asset Register (also known as an Information Asset Register);
- Identification and nomination of appropriately skilled individuals to undertake the role of IAA for each Information Asset;

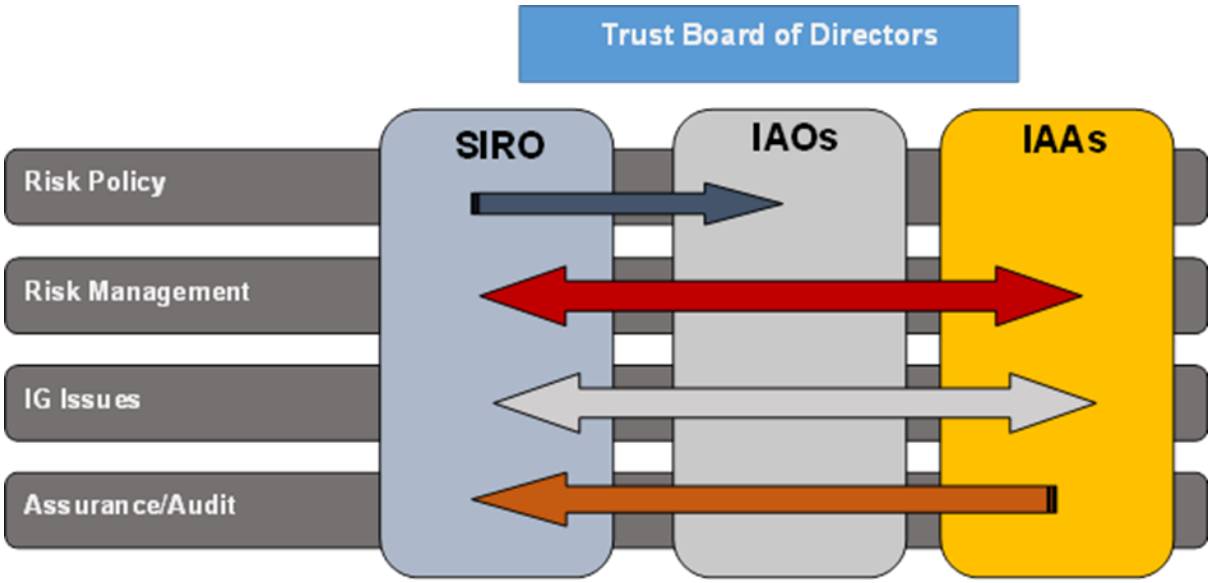
- Add the responsibilities of the IAA to the job description of the individual nominated (or otherwise ensure that the individual nominated as IAA is aware of their responsibilities associated with this role);
- Take ownership of their local control, risk assessment and management processes for the information 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.

9.2.2 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 5 – Communications SIRO, IAO, IAA



9.3 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.

9.3.1 IAAs' Responsibilities

IAA responsibilities are to:

- **Implement** the organisation's policies
- **Understand and address risks** to information assets, and provides assurance to the IAO
- **Ensure** compliance with 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 to maintain 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.

9.3.2 IAAs' 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 Contracts Manager to review the asset's 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 Wiltshire Health and Care's risk management system;
- Complete annual information risk management training.
- Undertake an assessment of the business importance/criticality of the asset to Wiltshire Health and Care.
- Record and maintain asset risks scoring over 8 within Wiltshire Health and Care'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.

10. Data Management

Wiltshire Health and Care 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, below, provides a pictorial view of lifecycle of data management within Wiltshire Health and Care.

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: 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.

11. 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 Wiltshire Health and Care. It allows Wiltshire Health and Care to get the maximum value and benefit from the system, equipment or application.

To provide assurance to Wiltshire Health and Care Board, Senior Information Risk Owner (SIRO) and Information Governance Policy and Oversight Group, the following IT asset management process has been introduced to ensure Wiltshire Health and Care 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 requires 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 planning and purchasing phase, then acquiring deployment, management (business as usual) disposal.

asset lifecycle management which starts at the the product, which naturally evolves into and eventually the retirement, archiving and

Compliance with the IT asset lifecycle procurement process controls, internal and reconciliation and asset disposal procedures.

management will be monitored through the external audit reports, the monitoring of

12. Freedom of Information and Environmental Information Regulations 2000

12.1 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 1 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, Wiltshire Health and Care is obliged to respond to all FOI requests for information within 20 working days. The process is managed by the Corporate Services team. Upon receiving a request, the Corporate Services team contacts relevant staff members that hold the information requested, and prepare a reply, which is signed off by a member of the Executive team before being sent on to the requestor.

With such a short timeframe, it is vital that all staff answer any queries as quickly as possible so that Wiltshire Health and Care is not in breach of its obligations.

12.2 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 Wiltshire Health and Care to make the distinction between Freedom of Information and Environmental Information Regulations and to respond accordingly.

Wiltshire Health and Care believes that as a public authority it must be allowed to discharge its functions effectively. This means that Wiltshire Health and Care 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.

13. Records Management / Information Lifecycle Management

Wiltshire Health and Care 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.

Wiltshire Health and Care 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 Wiltshire Health and Care 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.

14. 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 Policy and Oversight Group for approval prior to submission annually in March.

The Data Security and Protection Toolkit is an online self-assessment tool that permits Wiltshire Health and Care 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

15. Employees' 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, Senior Leaders, Heads of Service, Team Leaders and Ward Sisters 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.

A staff handbook has been developed to help all staff understand their roles and responsibilities around information governance across Wiltshire Health and Care (linked separately).

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 (linked separately).

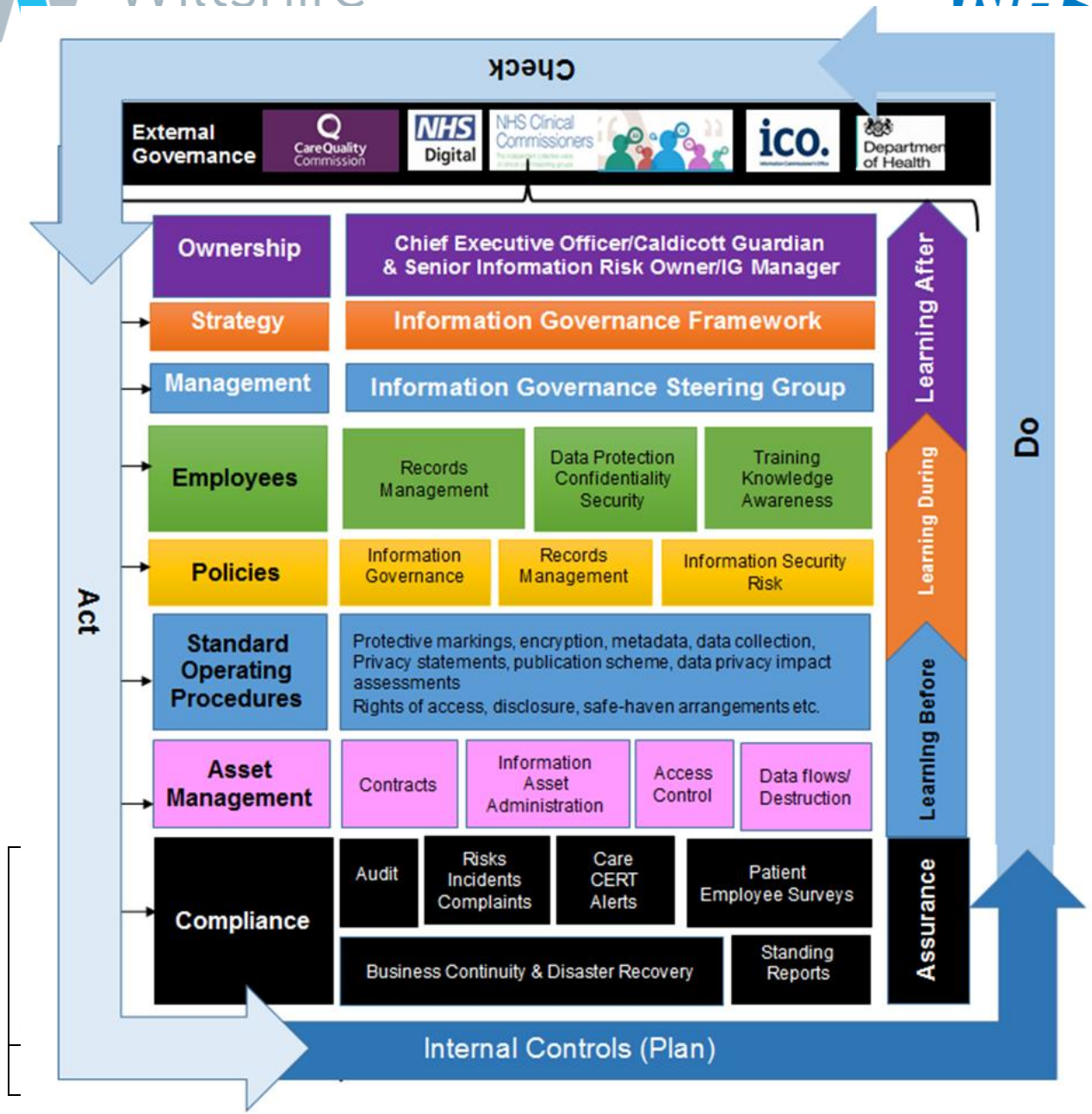
Section C – IG Standard Operating Procedures

Diagram 6 - 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.

Wiltshire

NHS



Appendices

(Employees' IG Handbook – separate document) – hyperlinked in due course

(Managers' IG Handbook – separate document) – hyperlinked in due course)

A. Equality Impact Assessment
B. Quality Impact Assessment
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

Appendix A – Equality Impact Assessment

There is a range of policies and procedural documents to support the implementation of equality and diversity within WHC, including the Equality & Diversity Strategic Framework.

Protected Characteristic	For employees	For patients
Age	Employment practices including recruitment, personal development, promotion, entitlements and retention encompass employees with protected characteristics.	• Services are provided, regardless of age, on the basis of clinical need alone. •
Disability -	Reasonable steps will be taken to accommodate the disabled person's requirements, including: • Physical access • Format of information • Time of interview or consultation event • Personal assistance • Interpreter • Induction loop system • Independent living equipment • Content of interview of course etc.	Reasonable steps are taken to accommodate the disabled person's requirements, including: • Physical access • Format of information • Time of consultation /event • Personal assistance • Interpreter • Induction loop system
Gender reassignment -	There is equal access to recruitment, personal development, promotion and retention. Confidentiality about an individual's gender status is	There is equality of opportunity in relation to health care for individuals irrespective of whether they are male or female.

	maintained.	Confidentiality about an individual's gender status is maintained and supported by a specific policy.
Marriage and Civil Partnership	There is equal access to recruitment, personal development, promotion and retention for individuals irrespective of whether they are single, divorced, separated, living together or married or in a civil partnership	There is equality of opportunity in relation to health care for individuals irrespective of whether they are single, divorced, separated, living together or married or in a civil partnership.
Pregnancy and Maternity -	There is equal access to recruitment, personal development, promotion and retention for female employees who are pregnant or on maternity leave. A woman is protected against discrimination on the grounds of pregnancy and maternity. With regard to employment, the woman is protected during the period of her pregnancy and any statutory maternity leave to which she is entitled. • There is a Flexible Working Policy.	There is equality of opportunity in relation to health care for women irrespective of whether they are pregnant or on maternity leave. A woman is protected against discrimination on the grounds of pregnancy and maternity.
Race - including Nationality and Ethnicity	There is provision for interpreter services for people whose first language is not English. Documents can be made available in alternative languages/formats Written communications are in plain English and the use of language particularly jargon or colloquialisms is avoided. Religion, belief and culture is respected.	There is provision for interpreter services for people whose first language is not English. Documents can be made available in alternative languages/formats Written communications are in plain English and the use of language particularly jargon or colloquialisms is avoided. Religion, belief and culture is respected.
Religion or Belief	HR policies cover consideration of: • Prayer facilities	Equality and Diversity guidelines enable consideration of:

	• Dietary requirements. • Gender of staff when caring for patients of opposite sex. • Respect for requests from staff to have time off for religious festivals and strategies. • Respect for dress codes	• Prayer facilities • Dietary requirements. • Gender of staff when caring for patients of opposite sex. • Respect for religious festivals • Respect for dress codes
Sex	HR policies cover consideration of: • Equal access to recruitment, personal development, promotion and retention. • Childcare arrangements that do not exclude a candidate from employment and the need for flexible working. • The provision of single sex facilities, toilets	Single sex facilities, including toilets and on wards, are provided.
Sexual orientation	HR policies cover consideration of: • Recognition and respect of individual's sexuality. • Recognition of same sex relationships in respect to consent. • The maintenance of confidentiality about an individual's sexuality. • Consider the effect on heterosexual, gay, lesbian and bi-sexual people	There is: • Recognition and respect of individual's sexuality. • Recognition of same sex relationships in respect to consent. • The maintenance of confidentiality about an individual's sexuality. • Consideration of the effect on heterosexual, gay, lesbian and bi-sexual people

Appendix B – Quality Impact Assessment Tool

Purpose To assess the impact of individual policies and procedural documents on the quality of care provided to patients by Wiltshire Health and Care
Process The impact assessment is to be completed by the document author. In the case of clinical policies and documents, this should be in consultation with Clinical Leads and other relevant clinician representatives. Risks identified from the quality impact assessment must be specified on this form and the reasons for acceptance of those risks or mitigation measures explained.
Monitoring the Level of Risk The mitigating actions and level of risk should be monitored by the author of the policy or procedural document or such other specified person. High Risks must be reported to the relevant Executive Lead.

Impact Assessment Please explain or describe as applicable.		
1.	Consider the impact that your document will have on our ability to deliver high quality care.	*The document will assist staff to deliver high quality care by setting out the legal framework around management of information, and by directing staff to a range of other documents to support this area of governance.*
2.	The impact might be positive (an improvement) or negative (a risk to our ability to deliver high quality care).	
3.	Consider the overall service - for example: compromise in one area may be mitigated by higher standard of care overall.	*This document will not compromise care in any other area*
4.	Where you identify a risk, you must include identify the mitigating actions you will put in place. Specify who the lead for this risk is.	

Impact on Clinical Effectiveness & Patient Safety		
5.	Describe the impact of the document on clinical effectiveness. Consider issues such as our ability to deliver safe care; our ability to deliver effective care; and our ability to prevent avoidable harm.	*The principles within the document are embedded alongside day-to-day collection and management of patient data.*
Impact on Patient & Carer Experience		
6.	Describe the impact of the policy or procedural document on patient / carer experience. Consider issues such as our ability to treat patients with dignity and respect; our ability to deliver an efficient service; our ability to deliver personalised care; and our ability to care for patients in an appropriate physical environment.	*The document allows patients to receive care from WHC, and referral to other services, correctly documented and securely saved.*
Impact on Inequalities, and Parity of Esteem		
7.	Describe the impact of the document on inequalities in our community. Consider whether the document will have a differential impact on certain groups of patients (such as those with a hearing impairment or those where English is not their first language).	*There should be no negative impact on any groups of patients.*

Appendix C: IG Training Needs Analysis for 2018-2020

Information Governance Training Needs Analysis

Who Needs IG Training - Job Role	What Training is needed	Introduction to IG (Year 1) Face to Face	IG-Refresher Module (Years 2 & 3)	The Caldicott Guardian in the NHS Linked to CPD	SIROs External Course CPD	NHS Information Risk Management IAOs	NHS Information Risk Management - Introductory	Access to Health Records	Records Management and the NHS Code of Practice Adhoc	Records Management in the NHS	Secure Transfers of Personal Data	Business Continuity Management	NEW-Access to Information & Information Sharing in the NHS -	NEW-Secure Handling of Confidential Information	Employment Code of Practice	NEW-Information Security Management	FOI Guardian	PDP Qualification
CEO	The Chief Executive will take full responsibility for the effective implementation of this IG Staff Training Strategy.	Mandatory	Mandatory				Recommended										Mandatory	
Deputy CEO	In the absence of the CEO - the deputy CEO will take full responsibility for the effective implementation of this IG Staff Training Strategy.						Recommended			Optional			Optional			Optional	Mandatory	
Senior Information Risk Officer (SIRO)	The SIRO will ensure the Trust Board is adequately briefed on all information risk issues associated with IG staff training. This will ensure:- • The Trust's approach in terms of resource, commitment and execution is effective and is communicated to all staff; • Ensure all training requirements are kept up to date.	Mandatory	Mandatory		Mandatory		Mandatory	Optional	Optional	Optional	Optional	Optional	Optional	Optional		Optional	Mandatory	
The Caldicott Guardian i.e. the Medical Director	The Caldicott Guardian will ensure all training requirements are kept up to date in line with changes in legislation and national NHS guidance.	Mandatory	Mandatory	Mandatory			Recommended						Optional	Optional		Optional		
The Deputy Director of IT and Informatics	The Deputy Director of IT and Informatics will take full ownership of this strategy and ensure its sits within the current Information Governance Framework.	Mandatory	Mandatory				Recommended			Optional		Recommended	Recommended	Optional		Recommended	Mandatory	
Head of Information and Data Quality	The Head of Information and Data Quality will ensure all the necessary risk assessments and training needs assessments have been conducted to ensure the effectiveness of the training programme is still fit for purpose.	Mandatory	Mandatory							Recommended			Mandatory	Mandatory		Mandatory	Mandatory	
Information Governance Manager	The Information Governance Lead will take full responsibility for the development and co-ordination of the Trust's IG staff training programme with O&D. This will involve reviewing and agreeing actions where information risks have been identified.	Mandatory	Mandatory	Mandatory			Mandatory			Mandatory		Recommended	Recommended	Mandatory		Recommended		Mandatory
Line Managers	Line Managers are responsible for ensuring that all IG communication and training requirements are cascaded to junior members of staff and all staff training sessions identified are attended to.	Mandatory	Mandatory				Mandatory			Recommended		Recommended	Optional	Recommended	Recommended	Optional		
IAO (Information Asset Owner)	IAOs are resonsible for information assets within their directorate of which they are designated as the owner	Mandatory	Mandatory			Mandatory	Mandatory					Recommended	Recommended	Recommended		Recommended		
IAA (Information Asset Admin)	IAAs are responsible for the day to day management of a system/asset	Mandatory	Mandatory			Recommended	Mandatory		Recommended	Recommended	Mandatory	Mandatory	Mandatory	Mandatory		Mandatory		
Records Manager	Records managers oversee an organisation's records from their creation and preservation through to disposal.	Mandatory	Mandatory				Mandatory	Mandatory				Mandatory	Recommended	Mandatory		Recommended		
Trust Staff - including Agency, locums, students, volunteers, trainees, temporary staff	All staff are expected to complete / attend their IG training sessions when requested.	Mandatory	Mandatory											Optional				
Cyber Security Staff	Protecting Information and data within the Trust and with other associated places.	Mandatory	Mandatory				Mandatory					Mandatory	Recommended	Mandatory		Recommended		
Governing Body/Trust Board	Ultimate responsibility for Information Governance in the Trust rests with the Board of Directors	Mandatory	Mandatory										Optional	Optional		Optional		
Medical Records Staff	Medical Records Staff atre responsible for managing all Trust medical records and dealing with SARs	Mandatory	Mandatory				Recommended	Mandatory					Optional	Recommended		Optional		
Directorate Managers/Head of Service Deputy	Senior Directorate and staff withinthat directorate. Making sure all staff are IG compliant	Mandatory	Mandatory				Recommended	Mandatory					Recommended	Recommended	Mandatory	Recommended	Mandatory	
Managers/Supervisors	Senior Directorate and staff within that directorate. Making sure all staff are IG compliant	Mandatory	Mandatory				Recommended	Mandatory	Optional	Mandatory		Recommended	Optional	Recommended	Mandatory	Optional		
IG Staff	Information Governance Staff	Mandatory	Mandatory				Mandatory			Mandatory		Recommended	Recommended	Mandatory	Optional	Recommended		Recommended

Appendix D - IG Standard Operating Procedure Structure

IG Standard Operating Procedure Structure Please note SOP's identified in red are currently under construction	
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
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 Libraries ○ Sharing of patient Healthcare Records to support transfer of patient care 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 ○ Complaints and Concerns ○ Information Governance Departmental Compliance Audit
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 SMS Text Messaging and Faxing 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 Directorate/Departmental non 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, WHCassets 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—
   (a) to obtain or disclose personal data without the consent of the controller,
   (b) to procure the disclosure of personal data to another person without the consent of the controller, or
   (c) 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.

2. It is a defence for a person charged with an offence under subsection (1) to prove that the obtaining, disclosing, procuring or retaining—
   (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.

3. 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 had a legal right to do the obtaining, disclosing, procuring or retaining,
   (b) 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
   (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 obtaining, disclosing, procuring or retaining was justified as being in the public interest.

4. 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.

5. It is an offence for a person to offer to sell personal data if the person—
   (a) has obtained the data in circumstances in which an offence under subsection (1) was committed, or
   (b) subsequently obtains the data in such circumstances.

6. 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.

7. In this section—
   (a) 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);
   (b) 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—
   (a) 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;
   (b) 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).

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

4. 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—
      (i) is the data subject to whom the information relates,
      (ii) had the consent of that data subject, or
      (iii) 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—
      (i) is the controller responsible for de-identifying the personal data,
      (ii) had the consent of that controller, or
      (iv) would have had such consent if that controller had known about the re-identification and the circumstances of it,

   (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 re-identification was justified as being in the public interest, or

(d) 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—
   (a) 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).

6. 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.

7. 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.

8. In this section—
   (a) 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);
   (b) 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.

3. 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.

4. 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.

2. 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).

3. 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.

4. 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.

5. 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

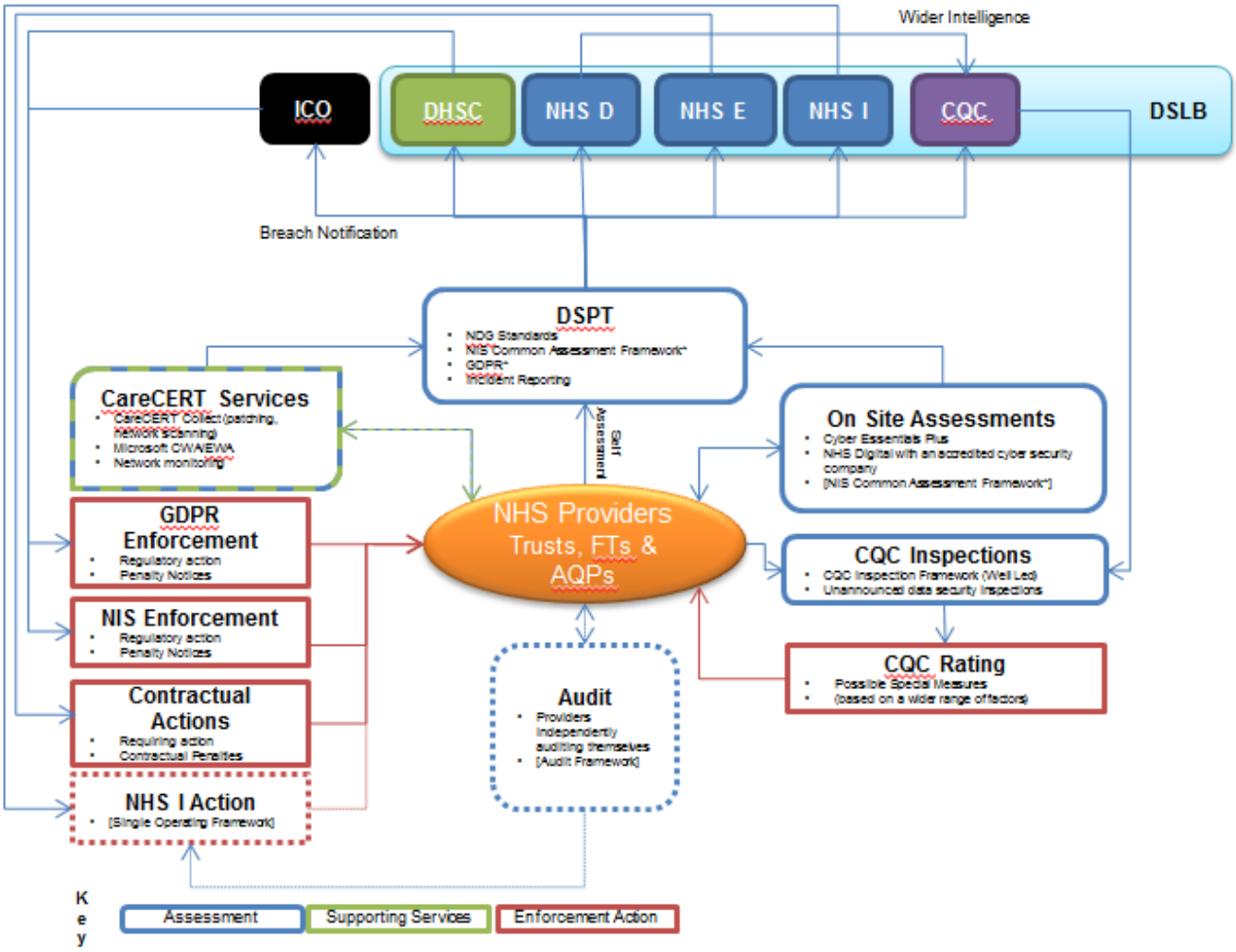
You may be breaching the Freedom of Information Act if you do any of the following:

- 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 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.

National Data Guardian

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.

Department of Health & Social Care

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

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

Care Quality Commission

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

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

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.

THE NETWORK AND INFORMATION SYSTEMS REGULATIONS 2018 (UK)

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

Privacy and Electronic Communications Regulations

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 to £500,000.