The Tavistock and Portman
NHS Foundation Trust

Information Governance and Data Security & Protection Management Framework

Version:	V1.1
Bodies consulted:	IG Workstream
Approved by:	EMT
Date approved:	September 2019
Lead manager:	Assistant Director of IG and Data Security
Responsible director:	SIRO (Deputy Chief Executive & Director of Finance)
Date issued:	September 2019
Review date:	September 2021
Intranet	Yes
Extranet	Yes

Contents

1 Introduction 3
2 Principles of Information Governance 4
3 Scope 5
4 Strategic Aims 6-8
5 Duties and Responsibilities 9-14
6 Supporting Policies 15
7 Monitoring and Review 15
8 References 16
9 Appendix 1 17
10 Appendix 2 18

Information Governance Management Framework

1. Introduction

1.1. Information Governance (IG) / Data Security and Protection (DSP) is the way in which an organisation processes or handles information, including person-identifiable data, corporate information and business data. Information plays a key part in the Trust (Tavistock and Portman NHS Foundation Trust) governance arrangements, and the quality of service planning, performance measurement, assurance and financial management relies upon accurate and available information.

1.2. Robust IG/DSP requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

1.3. This Information Governance Management Framework (IGMF) sets out how the Tavistock and Portman NHS Foundation Trust will deliver against these requirements.

1.4. Standards for IG/DSP and the management of information risk are incorporated into the NHS Data Security and Protection Toolkit (DSP). This is an online tool that enables organisations to measure their performance against data security assertions/requirements which reflects legal rules and Department of Health policy and covers all aspect of information governance / data security and protection, including:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Corporate Information Assurance
- Secondary Use Assurance

1.5. An annual self-assessment against the requirements or assertions of the DSP will be completed, which will enable the Trust to plan and implement standards of best practice and to measure and report compliance. The Trust will aim to achieve full evidenced compliance with all the assertions assessments against all the toolkit criteria, which represents legal and NHS requirements and best practice for handling personal and confidential information.

1.6. The trust will also ensure that all organisations that they have contracted to provide clinical services also achieve a satisfactory level of compliance with DSP assertions. This will be monitored via Data Security and Protection Toolkit, replacing the former IG Toolkit.

1.7. The DSPT is an NHS provided framework that therefore focussed on the best practices regarding processing of clinical data. Despite this constraint the DSPT does provide assurance against all aspects of information governance and data security legislation. While our education and training systems and data are not explicitly covered by the DSPT and will not be reported, the framework will be used internally to ensure equally high standards are maintained for our non-clinical data and information.

2. Principles of Information Governance / Data security

2.1. The four key strands to information governance are:

- Openness
- Legal compliance
- Information Security
- Information quality assurance

2.2. The Trust recognise the need for an appropriate balance between openness and confidentiality in the management and the use of information. The trust fully supports the principles of corporate governance and recognise their public accountability to safeguard, both personal information about patients, staff, student and commercially sensitive information

2.3. The Trust also recognise the need to share patient, students and staff information with other health organisations, Universities and government agencies like HMRC respectively in a controlled manner consistent with the interest of the patient and, in some circumstances the public interest. This provides assurance that information is dealt with legally, securely, efficiently and effectively. In order to deliver the best possible care.

2.4. The trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision-making processes.

2.5. The Trust will establish and maintain policies and procedures to ensure compliance with requirements contained in the NHS DSP toolkit

2.6. It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management across the following legislation and work areas

- The General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- Information Security Standard: ISO/IEC 27002:2005
- The NHS Care Records Guarantee for England
- The Social Care Records Guarantee for England
- Health and Social Care Records Management Code of Practice 2016
- Caldicott Guidance (including the Caldicott2 review "to share or Not to share" 2013
- Public Records Act 1958
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- National guidance and best practice from the Information Commissioners Office
- Human Right Act article 8
- The Record Management NHS code of Practice
- National Data Guardian "Review of Data Security Consent and Opt Outs" July 2016
- Department of Health "2017/18 Data Security and Protection for Health and Social Care Organisations"

3. Scope

3.1. This Information Governance / Data Security and Protection Management Framework applies to:

- **Systems** – The Trust systems, include, but are not limited to discrete systems such as those holding information relating to patients, students, finance, risk, complaints, incidents, freedom of information request, human resources, payroll, subject access request; less technical systems such as excel spreadsheets held on the network, and paper-based systems such as complaints files.

- **Information** – All information collected or accessed (electronic and paper based) in relation to any of the Trust activity whether by Trust staff or individuals and organisation under a contractual relationship with the Trust and all information stored on facilities owned or managed by the Trust or on behalf of the Trust. All such information belongs to the Trust unless proven otherwise.

- **Staff** – All staff, including Trust employees and non-employees who work within the Trust or its pilots' sites or under contract to them. This includes, but is not limited to, staff on secondments, students on placement, and people working in a temporary capacity

4. Strategic Aims

4.1. The aim of this Information Governance Management Framework is to set out how the Trust will effectively manage Information Governance. The Trust will achieve compliance through delivery of the following commitments:

4.2. Openness:

- Non-confidential information relating to the Trust and the services it commission will be available to the public through a variety of media.

- The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000.

- Patient, students and staff will have ready access to information relating their health care, their options for treatment and their rights as patients, students and staff.

- Clear information will be provided to patient and their families and carers about how their personal information is recorded, handled, stored and shared.

4.3. Compliance with legal and Regulatory Framework:

- The Trust will establish and maintain policies to ensure that compliance with all relevant legal and regulatory framework is achieved, monitored and maintained.

- The Trust will regard all identifiable personal information relating to patients, students and staff as confidential, and as such, take steps to ensure that the handling of such information complies with the GDPR and the Data Protection Act 2018 (except where there is a legal requirement to override the Act).

- The Trust will establish and maintain policies and procedures for the controlled and appropriate sharing of patient, students, and staff information with other agencies, taking account of all relevant legislation. This will include the completion of Data Protection Impact Assessments for all new systems, data flows and services to determine whether there is any potential impact on the information security, confidentiality or integrity prior to implementation.

- The trust will ensure that the requirement for good information Governance standards is embedded with all services specifications and contracts.

4.4. Information Security

- The Trust will establish and maintain policies and procedures for the effective and secure management of its information assets and resources. This will include the maintenance of an Information Asset Register held locally by the Trust.

- Robust arrangements for the assessments and management of information risks will have been established.

- The Trust will ensure that their Information Technology provider has appropriate policies and procedures to ensure the maintenance, monitoring and review of network security controls. These will include encryption controls, access controls, anti-virus / malicious code detection. Removal and prevention procedures, and environmental controls to protect network equipment.

- The Trust will ensure that all flows of person identifiable and sensitive information have been identified, mapped and risk assessed to confirm appropriateness and ensure security of the data transfer.

- The Trust will ensure that business continuity plans are up to date and tested for all critical information assets to ensure that information required for operational purposes is held securely and is available to and able to be accessed by those who need it.

- The trust will maintain and review appropriate incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

- The trust is committed to the use of pseudonymised and anonymised data wherever possible for contract monitoring purposes.

4.5. Information Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance and effective management of records.

- Information will be organised and managed in accordance with mandated and statutory standards and kept confidential where appropriate.

- The integrity of information will be assured, monitored and maintained, to ensure that it is of quality and reliable for use for the purpose that it is collected and used.

4.6. Staff Education, Training and Awareness

- The Trust recognise that Information Governance and Data Security education, training and awareness are essential for developing and improving staff members' information governance knowledge and skills. Data Security Awareness training must extend beyond basic confidentiality and security awareness in order to develop and follow best standards of practice. Staff need to understand the value of information and their responsibility for it, including data quality, information security, record management, confidentiality, legal duty, information law, rights of access and patients' rights in terms of right of privacy and choice.

- Data Security Standard 3 in the Caldicott 3 Review requires that all staff undertake appropriate annual data security training and pass a mandatory test. Therefore, if non-permanent staff have access to personal information they also need to complete annual training.

- The Trust have classified Data Security Awareness Level 1 training as mandatory for all staff, whether permanent, temporary or contracted, and students who are enrolled to courses that will require access to patients and the patient record. All new starters will be provided with Data Security Awareness Level 1 training as part of their induction programme, with refresher training being required on an annual basis. Training will mainly be delivered via ESR and the NHS Digital Online Tool. However, alternative training method such as face-to-face sessions will be available on request.

- Information Governance and Data Security will form part of the Trust induction process with a foundation presentation provided by the Assistant Director of IG and Data Security (or their delegate).

- Information Governance and Data Security will form part of the Trust INSET process with a refresher presentation provided by the Assistant Director of IG and Data Security (or their delegate), to include updates to policies, procedures and guidance.

- A training need analysis will be completed in order to identify the additional training requirements specific to the roles.

- The Trust is committed to sustain an effective organisational culture through the provision of clear advice and increased awareness and promotion of information governance requirements. In addition to annual training, this will be achieved through ongoing staff briefings. This will highlight the importance of complying with the organisation's information governance policies, procedures and guidance, including the consequences of failing to comply.

5. Duties and Responsibilities

5.1. Key forums and individuals with overarching responsibility for addressing the Information Governance agenda are detailed below. Individuals responsible for specific information governance roles, such as data protection, information security and data quality, are detailed in the organisation's relevant information governance policies.

5.2. Governing Body

Ultimate accountability for Information Governance rest with the Trust Board, which must ensure that it receives an appropriate level of assurance in relation to the Information Governance duties that it has delegated to the Information Governance Workstream via the Clinical Quality, Safety and Governance Committee and key officers. In particular it must ensure that:

- Details of serious incidents requiring investigation involving actual loss of personal data or breach of confidentiality are published in the Trust annual reports and reported to the Information Commissioner's Office in line with its national notification guidance. Serious incidents requiring investigation which are graded level 2 or above as per NHS Digital's *'Guidance for reporting, managing and investigating Information Governance Serious Incidents requiring Investigation'* must be reported via DSP incident reporting Tool.

- Any shortfalls in the requirements of the DSPT are being addressed.

5.3. Clinical, Quality, Safety and Governance Committee (CQSGC)

The CQSGC duties are to:

1) Ensure that appropriate comprehensive information governance framework and systems are in place throughout the Trust and its other sites in line with national standards.

2) Receive regular action plans with regard to the Trust progress on annual Data Security and Protection Toolkit submission.

3) Ensure that information is effective managed, and that appropriate policies, procedures and management accountability are provided and approved in relation to confidentiality, security and records management.

4) Ensure that information risks are identified, assessed and managed in line with the Information Governance Assurance Framework and recommend actions to the Trust Senior Information Risk Owner (SIRO) to ensure risks are mitigated.

5) Ensure that information incidents for commissioned services, are identified and managed in line with the National Serious Incidents Framework. This will include incidents that result in serious breach in confidentiality or data loss.

6) Assure the Trust Governing Bodies that all person identifiable information is processed in accordance with GDPR and the Data Protection Act 2018 and that all staff are aware and comply with the NHS code of confidentiality and other professional codes of conduct.

7) Ensure that new proposed changes to organisational processes or information assets are identified and risk assessed, considering any impact on information quality and identifying any new security measures that may be required.

8) Provide oversight and monitoring of the Trust DSP Toolkit compliance and advising the relevant Quality Scrutiny Panels regarding any areas of concern.

9) Ensure that all locally-developed clinical information systems are accredited and signed off by the Clinical Safety Officer as laid out by statute and the relevant Information Standard Notices.

10) Receive regular compliance reports on the processing of Freedom of Information Request; determining exemptions as appropriate

11) Develop an information governance training programme and monitor the progress of the staff training and awareness in line with the National Department of Health and Social Care requirements

12) Support the Caldicott function, working with the Caldicott Guardian to ensure work related to confidentiality and data protection is appropriately carried out and any risks reported appropriately.

13) Work with dependent contractors and commissioned services to ensure their compliance with the DSP Toolkit.

5.4. Chief Executive Officer

Locally the Chief Executive Officer has overall responsibility for each organisation's Information Governance Management Framework and has established the following management arrangements to ensure that it is implemented effectively.

5.5. Caldicott Guardian

The Caldicott Guardian is a senior clinician responsible for:

- Overseeing the development and implementation of those policies and procedures designed to ensure that all routine use of person-identifiable information is identified, justified, documented and monitored

- Overseeing the development and implementation of criteria and process for dealing with ad hoc requests for use of person-identifiable information for non-clinical purpose.

- Ensuring standard procedures and protocols are in place to govern access to person-identifiable patient information.

- Providing advice and guidance where required to the organisation's research and clinical audit processes and personnel to ensure protocols for releasing information for research and audit are in line with applicable Information Governance standards.

- Have oversight of the implementation of the revenant recommendations as outlined in the Caldicotts2 review 'To share or Not to Share' April 2013.

5.6. Senior Information Risk Owner (SIRO)

The SIRO is a Trust Board member responsible for ensuring that organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist to support the role of the SIRO.

The SIRO's responsibilities can be summarised as:

- Leading and fostering a culture that values, protects and uses information for the success of the Trust.

- Owning the Trust's overall information risk policy and risk assessment processes, ensuring they are implemented consistently by Information Asset Owners and agreeing action in respect of any organisational risks.

- Owning the Trust's information incident management framework, ensuring that the Trust approach to information risk management is effective in terms of clear lines of responsibilities and accountability,

resources, commitment and execution and that this approach is communicated to all staff.

- Ensuring that effective mechanisms are established and publicised for responding to and reporting perceived or actual serious IG incidents.

The SIRO is required to undertake information risk management training at least annually to ensure their skills and capabilities are up to date and relevant to the needs of the Trust.

The SIRO is also required to maintain sufficient knowledge and experience of the Trust's business and goals with particular emphasis on the use of and dependency upon internal and external information assets.

5.7. Data Protection Officer (DPO)

The Data Protection Officer (DPO) for the Trust cannot be dismissed or penalised for performing his/her related tasks, does not receive any instruction from the Trust regarding exercising GDPR duties and is bound by secrecy and confidentiality. The DPO is allowed direct access to the Trust Board in matters that relates to data protection. They will:

- Inform and advice on GDPR and related obligations
- Monitor compliance with GDPR and related obligations (including awareness raising and training)
- Provide advice about data protection impact assessment and to monitor its performance.
- Cooperate with supervisory authority (currently the Information Commissioner's Office (ICO).
- Act as a contact point for the supervisory authority (ICO)

5.8. Assistant Director of IG and Data Security

The Assistant Director of IG and Data Security leads the work with the Information Governance Workstream, supported by the nominated information governance officers, such as Information Asset Owners, within the Trust. Together, they are responsible for ensuring the effective management, accountability, compliance and assurance for all aspects of Information Governance.

Key responsibilities include:

- Ensuring that IG targets and expectations, both internal and external, are met, specifically bringing together and prioritising work on

initiatives including data protection, Caldicott principles, information Lifecyle management, and information security.

- Records storage, archiving and security, and ensuring that the organisation complies with the requirements for mapping information flows and other records management initiatives.

- Supporting the work of the Caldicott Guardian and the SIRO

- Identifying and reporting Information Governance risks.

- Providing advice and guidance on all aspects of IG and on all matters related to the Data Protection Act 2018, GDPR and related legislation.

- Developing and maintaining comprehensive and appropriate documentation that demonstrate commitment to, and ownership of, Information Governance responsibilities, such as the Information Governance Management Framework and associated policies and procedures.

- Ensuring that appropriate training is available to all staff and delivered in line with mandatory requirements.

- Maintaining a level of expertise required in order to deliver guidance and awareness to staff.

- Ensuring (through implementation of the Information Governance Management Framework and associated Information Governance Policies) that all staff employed by the Trust (including agency staff, individuals on honorary contracts, management consultants and students who use and have access to information) understand their responsibilities for Information Governance and comply with the law.

- Ensuring that DSPT returns are completed and reported to the CQSGC for approval.

- Supporting the CQSGC to discharge its Information Governance responsibilities.

- Providing advice and guidance to commissioning staff regarding tendering and procurement processes to ensure that all services and contracted services have robust Information Governance in place.

- Periodically reviewing the Trust inventory of Information assets.

5.9. Information Assets Owners (IAOs)

Information Asset Owners have been identified for each Information Asset. They will:

- Lead and foster a culture that values, protects and uses information for the success of the Trusts and for the benefits of the population/s.

- Understand the nature and justification of the information flows to and from information assets, which will support ongoing work to identify flows of person identifiable information.

- Know who has logical access to the asset and why, whether it is a system or information, to ensure access is monitored and compliant with relevant legislation and guidance.

- Understand and address risks to the asset and provide reporting and assurance to the SIRO.
- Complete and or attend training around information asset management and responsibilities.

5.10. Information Asset Administrators (IAAs)

Traditionally the Information asset management structure has IAO's supported by Information Asset Administrators (IAA's). IAA's would ordinarily be operational staff with day to day responsibility for managing risks to their information assets.

It is recognised that due to the small number within the Trust this structure of accountability would not necessarily work and therefore the key link will be between the SIRO and the IAO's. However, where possible an IAA will be identified for each information asset.

The Director of Technology and Transformation with the support of the Transformation Manager and Data Security and Protection Manager will provide an integrated information asset management risk report to the CQSGC.

IAO's will in any event seek support from staff with their area with regards to the day to day management of information assets.

5.11. All Staff

All staff, whether permanent, temporary or contracted, must be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, information security management and information quality.

6. Supporting Policies

6.1. The Information Governance Management Framework is supported by, and should be read in conjunction with the suite of Information Governance policies and procedures established by the Trust to provide comprehensive guidance on the Information Governance agenda and the responsibilities of its staff, including:

- Data Protection Procedure
- Information Governance Policy
- Information Security Policy
- Pseudonymisation and Anonymisation Procedure
- Record Management Schedule
- Freedom of Information Policy
- Data Quality Policy
- Data Sharing Procedure
- Access to Health Record Procedure
- Incident Reporting and Management Policy
- Internet and Electronic Policy
- Acceptable User Policy (AUP)

7. Monitoring and Review

7.1. This Information Governance Management Framework will be reviewed accordingly. Compliance with the Information Governance Management Framework will be monitored by the CQSGC which will oversee the production and delivery of an annual improvement plan.

7.2. An annual report detailing levels of compliance will be presented to the CQSGC.

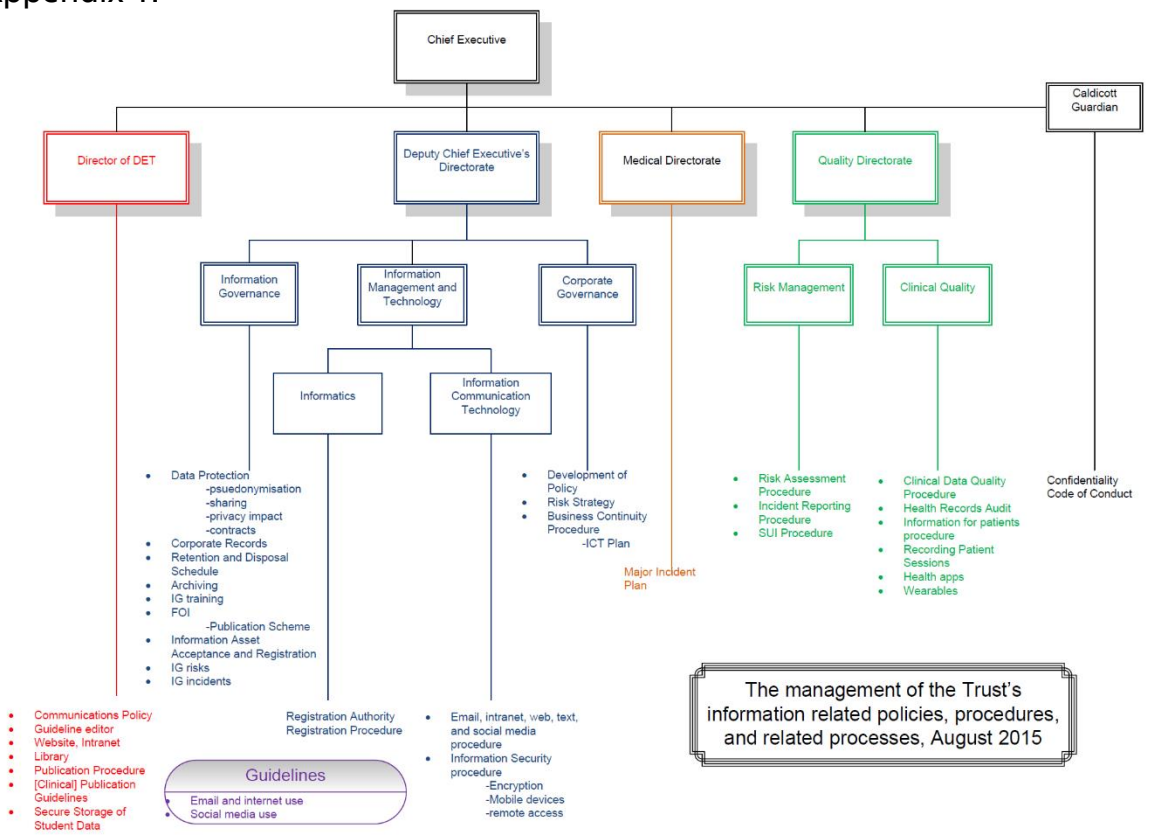
8. References

- NHS Digital Data Security and Protection Toolkit
- Information Commissioner's Office
- National Information Governance Board for Health and Social Care
- NHS Care Record Guarantee
- Data Handling Review (Cabinet Office 2012)

- Confidentiality: NHS code of Practice (Department of Health and Social Care 2003)
- Information Security management: Code of Practice
- Health and Social Care Records Management Code of Practice (2016)
- NHS Information Risk Management (Digital Information Policy, Dh, 2009)
- Caldicott2 Review 'To share or not to share' April 2013
- NHS Digital's A guide to Confidentiality' 2013
- Caldicott 3 Review
- The NDG Review (review of Data Security, Consent and Opt-Outs) July 2016
- Data Security and Protection Toolkit
- Department of Health ''2017/18 Data Security and Protection for Health and Care Organisations''

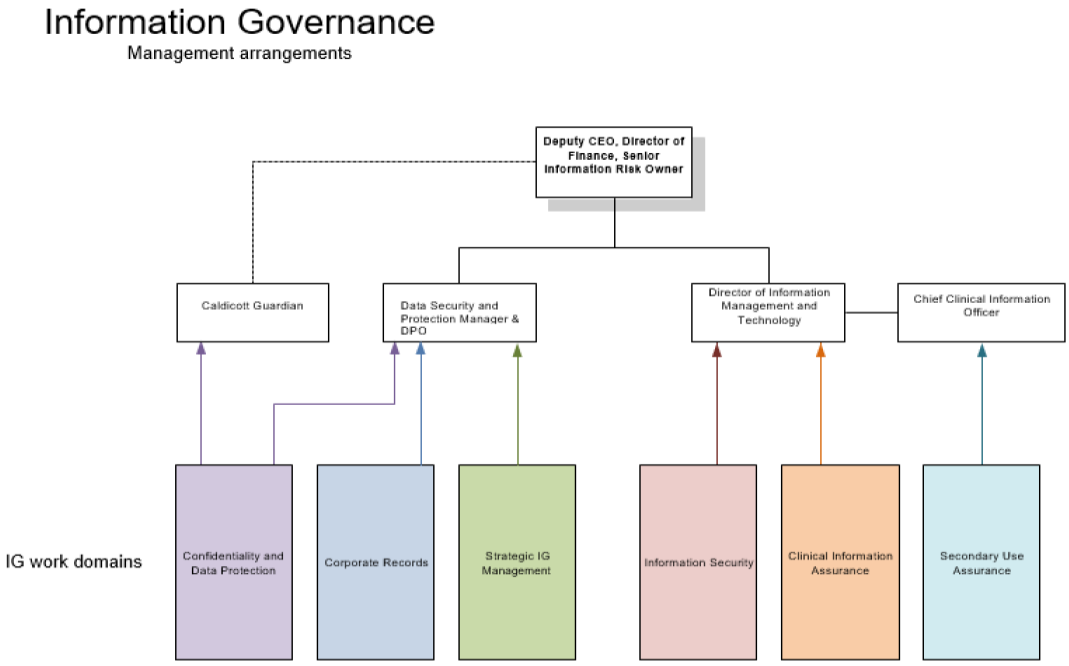
9. Appendix: Information Governance Management Framework Structure.

Appendix 1.



Reviewed September 2019

Appendix 2.



Completed by	**S.I Ndumbe**
Position	**Data Security and Protection Manager & DPO**
Date	**01st Oct 2018**

Reviewed Setpember 2019