Northern Ireland Ambulance Service
Health and Social Care Trust

1.0 **Title:**	**INFORMATION GOVERNANCE POLICY**		
2.0 **Author(s)**	Alison Vitty, Corporate Manager		
3.0 **Ownership:**	Finance and ICT Directorate		
4.0 **Date of SEMT Approval:**		5.0 **Date of Trust Board Approval:**	01/10/2015
6.0 **Operational Date:**	March 2016	7.0 **Review Date:**	01/10/2018
Version No:	Version 0.2.1	**Supersedes:**	No policy to supersede
8.0 **Key words:**	Information Governance		
9.0 **Other Relevant Policies:**	- Information Governance Strategy 2015-2018 - Information Risk Policy - Records Management Strategy - Records Management Policy - Freedom of Information Act 2000 and Environmental Information Regulations 2004		

Version Control for Drafts:			
Date	**Version**	**Author**	**Comments**
August 15	V0.1	AV	Initial draft.
September 15	V0.2	AV	Minor amendments made based on comments from Senior Information Risk Owner and Personal Data Guardian/Caldicott Guardian
September 15	V.0.2.1	AV	Minor amendments made based on consultation with Staff Side and Internal Management

1.0 INTRODUCTION

1.1 Information governance is the framework of law and best practice that regulates the manner in which information (including information relating to and identifying individuals) is managed, i.e. obtained, handled, used and disclosed.

1.2 The Northern Ireland Ambulance Service Health and Social Care Trust (NIAS) fully recognises and understands that having accurate, relevant and accessible information is vital to the efficient management of the organisation which values records and information as important corporate assets. The Trust is committed to applying the controls defined or referred to throughout this Policy (and associated Information Governance Strategy 2015-2018) to ensure compliance with legislation and good practice recommendations.

Effective information management will bring many benefits to the Trust by facilitating and supporting more efficient working, aid better decision making and improve patient experience. Without information the Trust would not be able to

- Manage individual patients and staff
- Plan day to day activities
- Manage the budget
- Contract with commissioners
- Develop services
- Monitor performance
- Satisfy the bodies that audit us Department of Health and Social Services (DHSSPS), Regulation Quality and Improvement Authority (RQIA)

1.3 Information governance (IG) within the Trust will aid:

- **Confidentiality –** confining the access to data with specific authority to view it.
- **Integrity –** safeguarding the accuracy and completeness of information and ensuring the correct operation of all systems, assets, processes and networks.

- **Accessibility –** ensuring that information is available and delivered to the right person, at the time when it is needed.
- **Authenticity –** ensuring information and records are credible and authoritative.
- **Reliability –** ensuring information and records can be trusted as a full and accurate representation of activities or facts.

This will assist the Trust in achieving:

Openness

- The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information as determined by law, stature and best practice.
- Personally identifiable information will be protected and managed according to the principles of Caldicott and outlined in the Data Protection Act.
- Non confidential information on the Trust and services will be available to the public through a variety of means, in line with the Freedom of Information Act.
- Patients will have access to information relating to their own health care, options for treatment and their rights as patients. There will be clear procedures and arrangements for handling queries from patients and the public.
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.
- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

Legal compliance

- The Trust regards all identifiable personal information relating to patients as confidential, compliance with legal and regulatory framework will be achieved, monitored and maintained.
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The Trust will establish and maintain policies and procedures to ensure compliance with the Data Protection Act, Human Rights Act, the common law duty of confidentiality, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and other associated legislative requirements.
- Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and appropriate training and awareness provided.
- Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable information governance controls are in place.

Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources.
- Audits will be undertaken or commissioned to assess information and IT security arrangements.
- The Trust will provide on Incident Reporting system to report, monitor and investigate all breaches of confidentiality and security.

Information Quality Assurance

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

- Audits will be undertaken or commissioned of the Trust's quality of data and records management arrangements.
- Managers throughout the Trust will be expected to take ownership of, and seek to improve, the quality of data within their services.
- Wherever possible, information quality will be assured at the point of collection.
- The Trust will promote data quality through policies, procedures/user manuals and training.

1.3 The Information Governance Assurance Framework (IGAF/"Framework") is a framework of standards that bring together all statutory, mandatory and best practice requirements concerning information management. The standards are set out in the Information Management Controls Assurance Standard as a road map enabling the Trust to plan and implement standards of practice and to measure and report compliance on an annual basis.

1.4 The Trust performance is mandated by and reported to the Department of Health and Social Services and forms part of the Trust's assurance processes.

2.0 GENERAL PRINCIPLES

2.1 "Information Governance" is an umbrella term for a collection of distinct but overlapping disciplines. Information Governance is about the way in which the Trust handles its information, particularly personal data. The Trust relies on good quality information being available at the point of need in order to aid decision making and provide a high quality service.

Staff rely on the quality of data they use to make decisions and the way in which we use resources and run the organisation. It is important for staff to understand their own responsibility for recording information to a consistently high standard and for keeping it secure and confidential, when required. Public confidence in our ability to handle data responsibly and efficiently is based on a good reputation for keeping data safe.

Information Governance has four fundamental aims:

- ✓ To support the provision of high quality care by promoting the effective and appropriate use of information;
- ✓ To encourage responsible staff to work closely together preventing duplication of effort and enabling more efficient use of resources.
- ✓ To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards.
- ✓ To enable the Trust to understand their own performance and manage and improve in a systematic and effective way.

2.2 Reference to information governance in this document shall also mean reference to the following but not exclusively limited to legislative, regulatory and Codes of Practices:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Access to Health Records (NI) Order 1993
- The Environmental Information Regulations 2004
- Privacy and Electronic Communications Regulations 2003
- The Public Records Act 1958
- Disposal of Documents Order 1925
- The Re-Use of Public Section Information Regulations 2005
- Computer Misuse Act 1990
- The Common Law Duty of Confidentiality
- The Human Rights Act 1998
- Electronic Communications Act 2000
- The Regulation of Investigatory Powers Act 1995
- BS ISO/IEC 27001:2005; ISO/IEC 27001:2013.
- ISO/IED 27001.
- DHSSPSNI Code of Practice on Protecting the Confidentiality of Service User Information 2012.
- The Personal Data Guardian Manual 2012.
- Information security assurance
- Information quality assurance.
- Records Management
- The ICO’s published guidance and codes of practice

Information Governance provides a consistent way for employees to deal with the many different information handling requirements.

2.3 This policy covers the use and management of information in all formats, including the collection, processing, storage, communication and disposal of information. This includes but is not limited to assets including:

- Corporate records
- Health and clinical Records
- Financial Records
- Staff Records
- Estates and Fleet Records
- Supplies and Stock
- Incidents, Complaints and Claims

The assets above are contained on manual and electronic datasets including (but not limited to):

- Corporate records held in Trust Board papers, minutes, Committee papers etc
- Health and clinical records - patient/client/service user information held on Command and Control system, Patient Report Forms (FORMIC), Voice Call Logger etc
- Staff Records e.g personnel files, HR Payroll, Travel and Subsistence (HRPTS), equality returns, Global Rostering Software (GRS), DATIX, Regional Ambulance Training Centre (RATC) – training records etc
- Estates Records held on 3i Estates Manager
- Supplies and Stock held on finance and procurement systems and manual filing systems
- Incidents, Complaints and Claims e.g DATIX

This policy applies to all aspects of information handling including but not limited to:

- Information recording and processing systems whether paper, electronic, video or audio records (including radio transmissions);
- Transmitted across networks whether internally or externally
- Disclosures of information, whether person identifiable, sensitive, confidential or corporate;
- Sent via email;
- Printed out and/or filed in some form;
- Written on paper and/or filed in some form;
- Sent by fax;
- Stored on tapes and disks;
- Captured on CCTV or digital camera;
- Spoken in conversation e.g. telephone;
- SStored on databases or bespoke software systems

This policy applies to all information systems purchased and/or managed by the Trust as well as the activities of any individual accessing the Trust's information assets.

3.0 **Compliance**

The Information Governance Assurance is measured via an annual assessment process of compliance against the standards set out in the DHSSPSNI Controls Assurance Standard on Information Management and is assured by Corporate Services. The Trust is also subject to internal audits in relation to the area of Information Governance and Information Technology which supports the IG Framework implementation.

4.0 **Statement of Compliance**

The Trust will aim to comply with all standards as laid out in the DHSSPSNI Information Management Control Assurance Standard and will seek to achieve and maintain substantive compliance on an annual basis.

5.0 **INFORMATION GOVERNANCE ROLES AND RESPONSIBLITIES**

5.1 **The Trust Board**

In his communications with Health and Social Care (HSC) Trust Chief Executives, the DHSSPS Health Minister and Permanent Secretary have made it clear that ultimate responsibility for information in the HSC rests with the Trust Board of the organisation, who should ensure that:

- Information governance is explicitly referenced within the Trust's Statement of Internal Control.

- A board-level Senior Information Risk Owner (SIRO) is required in the Trust and Senior Information Asset Owners should be designated from each Directorate area or other major information asset base.

- Appropriate information governance training is mandatory for all users of personal data and for all those in key roles.

- The IG Controls Assurance Assessment will continue with performance assessment on an annual basis. The results are made available to the public and reported in the Trust's Annual Report.

- Details of serious untoward incidents involving actual or potential loss of personal data or breach of confidentiality must be published in annual reports and reported to the DHSSPS and Information Commissioner as required.

- Refer to **Annex A** for Information Risk/Roles and Responsibilities with the Trust

5.2 Chief Executive

The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for IG in the Trust and is required to provide assurance through the Statement of Internal Control that all risks to the Trust, including those relating to information are effectively managed and mitigated. Serious Untoward Incidents involving data loss or confidentiality breaches must also be reported in the Annual Report.

5.3 Senior Information Risk Owner (SIRO)

The Director of Finance and ICT in the Trust is the Senior Information Risk Owner (“the SIRO”). The SIRO has overall responsibility for managing information risk across the Trust and is the owner of the Information Asset Register. The SIRO is a member of the Senior Management Team and the Trust Board and provides written advice to the Accounting Officer on the content of the Statement of Internal Control in regard to information risk. See **Annex B** for list of key responsibilities.

5.4 The SIRO is responsible to the Trust Board for ensuring that all Information risks are recorded and mitigated where applicable. The SIRO is responsible for ensuring that all record management issues (including electronic media) are managed in accordance with the Information Governance and Records Management Policies.

5.5 The SIRO owns the Trust’s overall information risk assessment process, tests its outcome, and ensures that it is used. The SIRO is responsible for how the Trust implements Information Governance risk management in its own services and activities and those of its delivery partners, and how compliance will be monitored.

The SIRO will ensure that information asset risk reviews are completed bi-annually. Based on the information risk assessment the SIRO will evaluate what information risks there are to the Trust and its business partners through its delivery chain, and ensures that they are addressed, and that they inform investment decisions including the risk considerations of outsourcing and how they may be reflected on the corporate risk register.

5.6 The SIRO is supported by Information Asset Owners (the “IAOs”) and the Information Governance Steering Group, although ownership of Information Risk and the information risk assessment process remain with the SIRO.

5.7 The Caldicott Guardian

The Trust is required to appoint a Caldicott Guardian to act as a focal point for patient confidentiality and information sharing issues and advising on options for lawful and ethical processing of information as required. The Chief Executive has appointed the Medical Director to this role.

5.7.1 Personal Data Guardian (PDG)

The Trust is required to appoint a Personal Data Guardian. The Chief Executive appointed the Medical Director to this role. The PDG ensures:

- Ensures that the Trust satisfies the highest practical standards for handling person identifiable information;
- Actively supports work to facilitate and enable information sharing, and advises on options for lawful and ethical processing of information as required;
- Has a strategic role, which involves representing and championing information governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the Trust's overall governance framework.

- The PDG is the conscience of the organisation in respect of personal and patient information and promotes a culture that respects and protects personal data. The PDG works closely with the SIRO and Information Asset Owners where appropriate, especially where information risk reviews are conducted for assets which comprise or contain patient/service user information.

5.8 **Information Asset Owner**

Information Asset Owners (IAOs) are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they have responsibility for. IAOs will also lead and help foster within their respective business areas a culture that values, protects and uses information.

5.9 IAOs must be a member of staff who is senior enough to make decisions concerning the asset and how it operates. The IAOs have responsibility for the completion and maintenance of the Trust's Information Asset Register and for providing assurance to the SIRO that information risks within their respective Directorate have been identified, recorded and controls are in place to mitigate those risks.

5.10 Their role is also to understand and assess risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They will ensure that all threats, vulnerabilities and impacts are properly assessed and included in local Information Asset Registers and where necessary the corporate risk register.

IAOs in conjunction with their Directors are responsible for ensuring:

- The IAO for the Directorate, when required, attends the Information Governance Steering Group;
- Appropriate Directorate structures are put in place to support the information governance agenda;
- Information governance issues are reported in accordance with the Trust's Risk Management Strategy and associated processes.

See **Annex C** for list of key responsibilities of IAO’s

5.11 Information Asset Assistants (IAAs)

The IAOs are responsible for appointing Information Asset Assistants (IAAs). It is at the IAOs discretion how many IAAs are appointed to support them in their role. Information Asset Administrators are operational staff with day to day responsibility for managing risks to their information assets. They will support IAOs by ensuring that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, ensure that privacy impact assessments are completed and ensure that information asset registers are accurate and up to date.

See Annex D for list of key responsibilities.

5.12 Directors and Senior Managers

Directors are responsible for managing this policy and working with IAOs and Senior Managers and other staff within Directorate areas to ensure robust information management and security measures are in place and are being complied with. This includes ensuring that permanent, temporary or third party suppliers are aware of:

- The information governance and security policies and procedures in their area;
- Their personal responsibilities for information governance and security;
- The development of local procedures within Directorate areas to ensure compliance with information governance.
- How to access advice on information governance

5.13 Caldicott Champion - Corporate Manager
Data Protection Officer – Corporate Manager
Freedom of Information Practitioner – Corporate Manager

The Corporate Manager is accountable to the Director of Finance and ICT and responsible for ensuring the development and implementation of this Policy and for the delivery of IGAF agenda.

The Corporate Manager will take day to day responsibility for developing, monitoring and overseeing the implementation of the IGAF policies and procedures including data protection, freedom of information, records management and providing the mechanisms for supporting access to information compliance.

The Corporate Manager also acts a Caldicott Champion supporting the Caldicott Guardian in his role.

The Corporate Manager also has the day to day role of the Data Protection Officer and is the Freedom of Information Practitioner responsible for ensuring that the organisation complies with all aspects of the Freedom of Information 2000 including the Publication Scheme and the processing of all formal requests for information.

5.14 All Staff

All NIAS employees and anyone else working for the Trust e.g agency staff, voluntary services, contractors, suppliers etc who use and has access to Trust information must understand their personal responsibilities for information governance and comply with the Law.

It is the responsibility of all staff to make themselves familiar with and comply with policies and procedures issued by the Trust, and aware that failure to comply may result in disciplinary action. All staff will work within the principles outlined in the Information Governance framework and undertake information governance training at point of induction and a three yearly basis.

5.15 Information Governance Steering Group (IGSG)

The Information Governance Steering Group has responsibility for overseeing the implementation of this Strategy, the Information Governance Policy and relevant IG Deliverable Programmes of work, the annual Information Management Control Assurance Standards assessment. The IGSG also reviews and recommends all IG related policies and procedures.

The IGSG reports to Trust Board through the Assurance Committee.

6.0 TRAINING AND AWARENESS

6.1 Fundamental to the success of delivering the IG Framework is developing an IG culture within the Trust. Awareness and training will be provided to all Trust staff who utilise information in their day-to-day work to promote this culture.

6.2 All staff will receive basic information governance training appropriate to their role through either face to face training, workbooks or an eLearning package.

6.3 IG Training is incorporated into the Trust's Training programme as it is a mandatory requirement for all staff in the Trust to undertake corporate induction (which include Information Governance) at point of entry and IG training once every three years or more frequently if required. This includes staff on temporary contracts, secondment, agency staff, students and volunteers.

6.4 Different levels of training will be delivered:

- All staff to receive Information Governance awareness training as part of their corporate induction programme.
- Internal training for staff who handle personal information as a routine part of their job provided by the Corporate Manager and/or Information Asset Owners.

- Internal and external Training for those engaged in, or intends to take on IG specialist roles e.g. SIRO (Senior Information Risk Owner), Personal Data Guardian, Caldicott Guardian, Information Asset Owners and Information Asset Assistants. A training matrix will be developed to support this.
- This includes all staff on temporary contracts, secondment, agency staff, students and volunteers.

7.0 <u>CODE OF CONFIDENTIALITY</u>

7.1 All staff, whether permanent, temporary, seconded, agency, students or volunteers should be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, information security management and information quality. Failure to maintain confidentiality, compliance with policies and procedures may lead to disciplinary action, up to and including dismissal.

7.2 The Trust will ensure that all stakeholders are adequately informed about confidentiality and the way their information is used and shared and their rights as data subjects. In particular this will cover how they may access their personal data and how they may exercise those rights when consent is required to use their data for non-healthcare purposes.

8.0 **INFORMATION RISK**

8.1 The Trust will establish clear lines of accountability for information risk management that lead directly to the Trust Board through the SIRO and the appointment of IAOs and IAAs.

8.2 The IAOs will be accountable through their director and the SIRO to the Accountable Officer, the Chief Executive for the management and mitigation of information risks and will provide assurance to that effect for the Annual Report and Statement of Internal Control.

8.3 The IAO will ensure that information risk assessments are performed at least twice each year on all information assets where they have been assigned ‘ownership’ of. They will ensure that any significant risks are included in a quarterly assessment to the SIRO.

8.4 Further information on the management of information risk, along with roles and responsibilities of individuals is available in the Information Risk Management Policy and Information Asset Register Process document.

An example of the Information Management Risk Assessment Template is contained at **Annex E**.

8.5 All appropriate risks will be entered onto the appropriate local risk register as documented in the Trust’s **Risk Management Strategy and Policy**. Further to this any severe risks will be reported to Senior Executive Management Team (SEMT) or IGSG for consideration and possible inclusion on the Corporate Risk Register.

8.6 The SIRO by means of the IGSG or earlier escalation plans will be made aware of all information risk assessments and approve identified risk mitigation plans.

8.7 On an annual basis the Trust’s IAOs will provide assurances to the SIRO on the security and use of assets they ‘own’.

9.1 Information Security Incident Management

9.1 The SIRO must be informed immediately of all information security incidents involving the unauthorised disclosure of person identifiable data/information for consideration of any necessary actions.

9.2 A key function of the IGSG is to monitor and review untoward occurrences and incidents relating to IG and to ensure that effective remedial and preventative action is taken. Reports of such incidents will be distributed to the IGSG for consideration.

9.3 Information incident reporting will be in line with the Trust's overall incident reporting processes. Please refer to the Trust's Risk Management Policy.

10.0 SECURITY OF INFORMATION

10.1 The Trust will protect personal data held in its information systems. Through compliance with the *DHSSPSNI: Code of Practice* on Protecting the Confidentiality of Service User Information and awareness of *ISO/IEC 27002:2013.*

10.2 Please refer to ICT Security Policy and Information Security Policy for more detailed guidance on encryption and access to service user information.

11.0 Privacy Impact Assessments

11.1 The impact of any proposed changes to the processes and/or information assets need to be assessed in accordance with the Information Risk Management Policy, to ensure that the confidentiality, integrity and accessibility of personal information are maintained.

11.2 The SIRO should be consulted during the design phase of any new service, process or information asset so that they can decide if a privacy impact assessment is required for a particular project or plan.

11.3 Refer to the Trust's Privacy Impact Assessment process for further information.

12.0 INFORMATION ASSET REGISTER

12.1 All assets should be clearly identified and a register of all assets drawn up and maintained.

12.2 It will be the responsibility of each IAO to identify what information assets are held within their area of responsibility, and to ensure this is documented in their Directorate's Information Asset Register which will form part of a Trust wide Register owned by the SIRO.

12.3 The asset register should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The register should not duplicate other inventories unnecessarily but it should be ensured that the content is aligned. In addition, ownership should be agreed and documented for each of the assets.

12.4 Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets should be identified as should details of risk assessor, risk assessment frequency, risk assessment rating and date of last risk assessment.

12.5 All information and assets associated with information processing facilities should be owned by a designated part of the Trust, e.g. a Directorate/Service area. **Priority must be given to information assets that comprise or contain person identifiable data/information.**

12.6 The IAO is responsible for ensuring that information and assets associated with information processing facilities are appropriately identified and classified; including defining and periodically reviewing access restrictions, classifications, and business continuity arrangements taking into account applicable access control policies.

12.7 Routine tasks may be delegated, e.g. to a custodian looking after the asset on a daily basis e.g IAA but the responsibility remains with the IAO.

12.8 In complex information systems it may be useful to designate groups of assets, which act together to provide a particular function as ‘services’. In this case the service owner is responsible for the delivery of the service, including the functioning of the assets, which provide it.

12.9 Refer to the Trust’s Information Asset Register Procedure for further guidance.

13.0 FREEDOM OF INFORMATION (FOI)/ENVIRONMENTAL INFORMATION REGULATIONS 2004

13.1 The Trust will ensure compliance with the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 and ICO guidance. This is set out in the Trust's Freedom of Information and Environmental Information Regulations 2004 Policy along with associated FOI Procedures.

14.0 CONFIDENTIALITY OF PERSONAL DATA

The Trust, as the "legal person" and Data Controller for the purposes of the Data Protection Act 1998 will ensure that all personal data it holds is controlled and managed in accordance with the terms of the Data Protection Act 1998 principles, European Convention of Human Rights (Article 8) (Human Rights Act 1998) and common law. This is set out in the Trust's Data Protection Policy and Records Management Policy and Strategy.

15.0 RECORDS MANAGEMENT

15.1 The Trust is committed to a systematic and planned approach to the management of records from their creation to their ultimate disposal. The Trust will ensure that it controls the quality and quantity of the information that it generates, can maintain that information in an effective manner and can dispose of the information efficiently when it is no longer required. This is set out in the Trust's Records Management Policy and Records Management Business Rules. It is also set out in "Good Management, Good Records" – DHSSPS Guidance adopted by the Trust.

15.2 To ensure that the Trust maintains the highest standards in the quality of its records an annual audit of corporate records will be undertaken.

16.0 **THIRD PARTY CONTRACTORS**

16.1 In day to day business, third parties gain access to information assets, e.g. computers, telephones, paper records etc. The third parties could include temporary agency staff, consultants, IT support staff, domestic staff, catering staff and security guards. It is possible that as a result of access to information assets, third party staff may have significant access to personal/ sensitive personal data. This situation therefore clearly has information governance risk implications such as data being used inappropriately.

16.2 Suitable clauses must be included when negotiating and completing contracts with third parties who have access to or process personal information on behalf of the Trust. All contractors with access to Trust's information assets should be clearly identified and appropriate information governance clauses included in their contracts. The terms and conditions of a contract must ensure that failure to deliver any aspect of information governance assurances will be at the third parties risk.

16.3 Attention should also be paid to the possible use of sub-contractors by the third party to provide services in order to undertake the contract.

16.4 The SIRO and IAOs must take all reasonable steps to ensure that that contractors used by the Trust to whom personal information is disclosed comply with their contractual obligations to keep personal information secure and confidential.

16.5 The BSO Directorate of Legal Services is to also ensure that all Barristers appointed as Counsel on behalf of the Trust have signed a suitable written undertaking with regards to Information Governance and that this is retained on file.

16.6 Risk Assessments

Directorates and IAOs should ensure that a risk assessment has been carried out prior to any agreement being made with a third party to evaluate any potential threats to networks, systems and locations from third party operatives. This should take into consideration the likelihood and consequence using the information risk assessment.

The ways in which third parties gain access, will help determine how extensive the risk assessment needs to be. For example, a risk assessment for cleaning contractors will be different to that carried out for a contractor connecting to the network. Temporary access will also see different considerations to long-term access. An Information Risk Assessment template can be located at **Annex E.**

16.7 Review of Contracts

IAOs should ensure that all existing contracts are monitored and reviewed annually to ensure that IG controls are being adhered to and to resolve problems or unforeseen events.

A register of all third party contracts should be maintained.

17.0 CONSENT TO SHARE INFORMATION

17.1 It is generally accepted that consent to disclose or to use patient information can be implied where the purpose is directly concerned with the individuals care or with the quality assurance of that care.

17.2 The Trust will share information in accordance with DHSSPS & HSC protocol for sharing service user information for secondary purposes.

18.0 INFORMATION SHARING AGREEMENTS

18.1 Sharing information about an individual between partner agencies is vital to the provision of co-ordinated and seamless services within HSCNI family and support patient and staff provision. The need for shared information standards and robust information security to support the implementation of joint working arrangements is recognised.

18.2 Routine information sharing requires the use of Data Access Agreements and information sharing protocols in order to ensure that the 'rules' are clearly understood and that the requirements of law and guidance are being met. Information sharing protocols are not required where the sharing is for an ad hoc request for information. On those occasions it is merely essential to ensure that the normal rules for the handling and disclosing of personal data are adhered to.

19.0 TRANSFERS OF PERSONAL INFORMATION OUTSIDE THE UK

19.1 The Data Protection Act 1998 governs transfers of personal information and requires that personal information is not transferred to countries outside of the European Economic Area unless that country has an adequate level of protection for the information and for the rights of individuals. The European Economic Area (EEA) is made up of the EU member states plus the European Free Trade Association (EFTA) countries of Iceland, Liechtenstein and Norway.

19.2 All transfers of personal data outside the EEA must be for a lawful and justified purpose and the Personal Data Guardian must be informed of such transfers. A log shall be maintained of such transfers.

19.3 Personal Information should only be transferred outside the EEA if the individual's consent, which should be explicit, has been obtained or following a risk assessment and the Personal Data Guardian is satisfied that there is an adequate level of protection in place. In certain circumstances a contract containing standard EU approved clauses as providing adequate protection to transfer individuals' personal information may be necessary

20.0 <u>INFORMATION GOVERNANCE DELIVERABLE/IMPROVEMENT PLANS</u>

20.1 Actions to ensure compliance with this policy are detailed in the Trust's Information Governance Strategy. The Strategy includes an Improvement Plan identifying key areas of work necessary to ensure compliance with this Policy. Formal reporting arrangements are also outlined with expected timeframes. Compliance with the Information Governance Assurance Framework will also be assessed by the annual completion of the Information Management CAS. Formal reports will be provided to the SIRO for sign-off prior to submission.

20.2 These plans will be used to determine the course of IG activity during the period and contain the following clearly defined areas.

- SMART objectives and deliverables
- What resources are available to deliver the plan
- Identified IG risks and issues that may impact upon delivery of the improvement plan.
- Key elements of the strategy should be delegated to specific members of the IGMG to ensure ownership.
- To provide a clear approval process through IGSG, SEMT and to the Trust Board all actions must be recorded on the IGSG Agenda and Minutes with the improvement plan remaining a standing agenda item.
- The Plan will be refreshed as required within year in response to non-forecasted events.
- Careful consideration must be given as to whether the plan is likely to intersect with any other Trust plans or strategies and if so steps taken to ensure adequate communication occurs so that the plans complement and enhance each other.

21.0 MONITORING/REVIEWED

This policy will be reviewed/monitored every three years or earlier, if affected by major internal or external changes such as:

- Legislation;
- Changing methodologies;
- Change in roles.

22.0 CONSULTATION PROCESS

- Senior Information Risk Owner/Caldicott Guardian: August 2015
- Senior Executive Management Team: September 2015
- Senior Information Risk Owners: September 2015
- Senior Managers throughout the Trust: September 2015
- Trade Unions: September 2015

23.0 APPENDICES/ANNEXES

Annex A:	Information Roles and Responsibilities within the Trust
Annex B:	Key Responsibilities of the Senior Information Risk Owner
Annex C:	Key Responsibilities of the Information Asset Owners (IAOs)
Annex D:	Key Responsibilities of the Information Asset Assistants (IAAs)
Annex E:	Information Risk Assessment Form
Annex F:	Information Governance Policy Framework

24.0 EQUALITY STATEMENT

24.1 In line with duties under Section 75 of the Northern Ireland Act 1998; Targeting Social Need Initiative; Disability Discrimination Act 1995 and the Human Rights Act 1998, an initial screening exercise to ascertain if this policy should be subject to a full impact assessment has been carried out.

24.2 The outcome of the screening exercise for this policy is:

Major Impact □

Minor Impact □

No Impact ☒

Still Being Determined □

25.0 SIGNATORIES

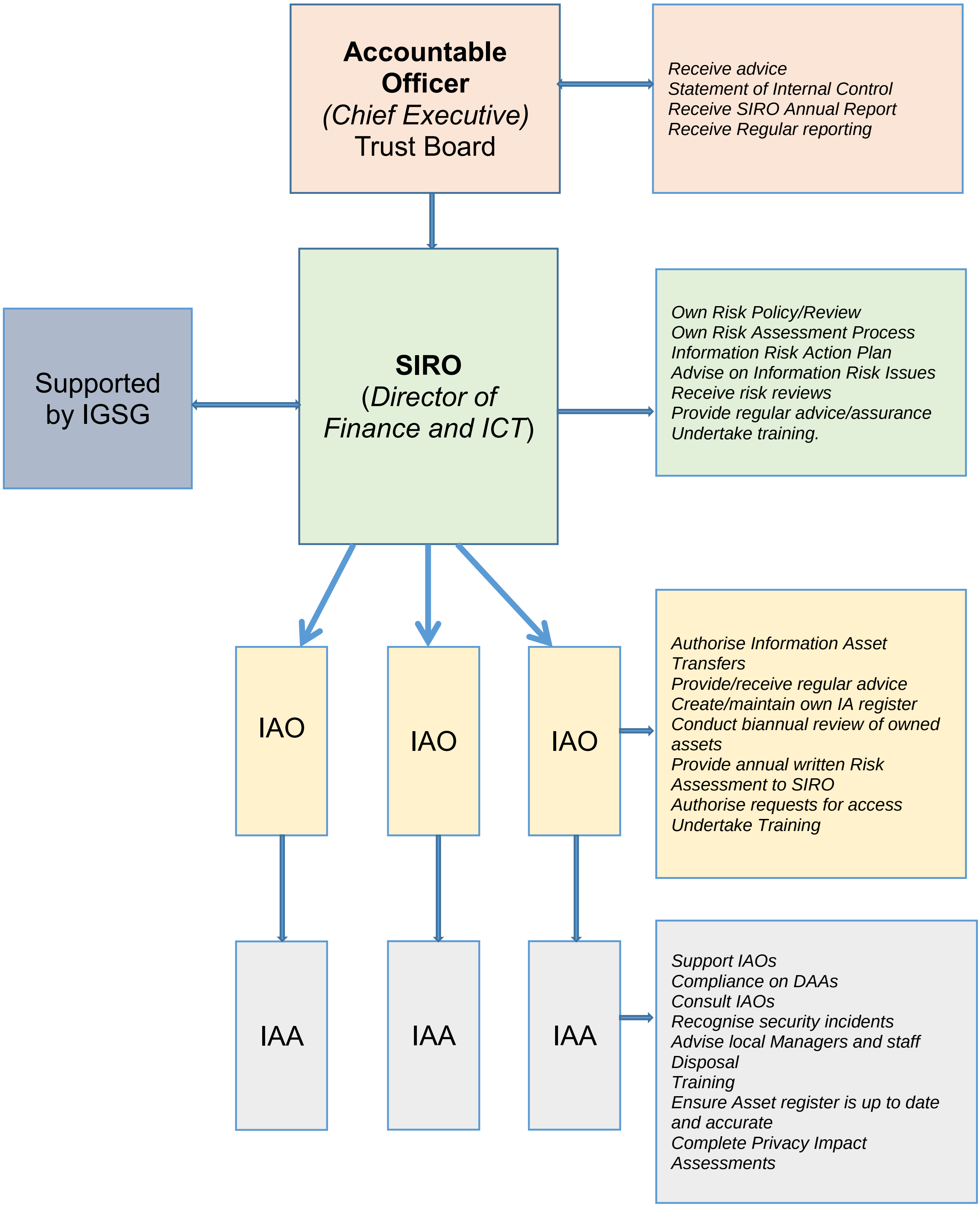
______________________________ **Date:** ____________________________

Lead Author

______________________________ **Date:** ____________________________

Lead Director

Annex A - Information Risk Roles and Responsibilities with the Trust



Accountable Officer
(Chief Executive)
Trust Board

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

Supported by IGSG

SIRO
(*Director of Finance and ICT*)

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

IAO

IAO

IAO

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

IAA

IAA

IAA

Support IAOs
Compliance on DAAs
Consult IAOs
Recognise security incidents
Advise local Managers and staff
Disposal
Training
Ensure Asset register is up to date and accurate
Complete Privacy Impact Assessments

Annex B - Key Responsibilities of the Senior Information Risk Owner (SIRO)

- To oversee the development of an Information Governance Strategy, Information Governance Policy and Information Risk Management Policy for implementing the policy within the existing Information Governance Framework.

- To take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.

- To review and agree an action plan in respect of identified information risks.

- To ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.

- To provide a focal point for the resolution and/or discussion of information risk issues.

- To ensure the Board is adequately briefed on information risk issues.

- To advise the Chief Executive and the Trust Board on information risk management strategies and provide periodic reports and briefings on IG improvements and progress.

Annex C - Key Responsibilities of the Information Asset Owners (IAO)

IAO Information Management Responsibilities

- To understand and address risks to the information assets they ‘own’ and provide assurance to the SIRO on the security and use of these assets (understands the Trust’s plans to achieve and monitor the right IG culture, across the Trust and with its business partners and to take visible steps to support and participate in that plan (including completing own training).
- Know what information the asset holds, and understands the nature and justification of information flows to and from the asset (approves and minimises information transfers while achieving business purposes; approves arrangements so that information put onto portable or removable media like laptops is minimised and are effectively protected to IG standards.
- Know who has access and why to your information assets. Ensure their use is monitored and compliant with policy (checks that access provided is the minimum necessary to satisfy business objectives; receives records of checks on use and assures self that effective checking is conducted regularly).
- Ensure the confidentiality, integrity, and availability of all information that their system creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO for review. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks.
- Ensure the asset is fully used for the benefit of the Trust and its patients, including responding to requests for access from others (considers whether better use of the information is possible or where information is no longer required; receives, logs and controls requests from others for access; ensures decisions on access are taken in accordance with IG standards of good practice and the policy of the Trust).
- Approve and oversee the disposal mechanisms for information of the asset when no longer needed

  .

- In the context of records management and information quality, working with local management, IAOs will ensure that staff accessing and using an Asset are fully trained in record creation, use and maintenance, including having an understanding of:
    - What they are recording and how it should be recorded;
    - Why they are recording it;
    - The need to differentiate fact from opinion and how to represent information supporting the opinion;
    - How to validate information with individuals or against other records – to ensure that staff are recording the correct data;
    - How to identify and correct errors – so that staff know how to correct errors and how to report errors if they find them;
    - The use of information – so staff understand what the records are used for (and why timeliness, accuracy and completeness of recording is so important); and
    - How to update information and add information from other sources.

IAO Assurance & Reporting Responsibilities

- Ensure all Information Assets are recorded on the Information Asset Register and the register is reviewed every six months.
- Understand and address risks to the asset, and provide assurance to the SIRO by completing an Information Risk Assessment (makes the case where necessary for new investment or action to secure 'owned' assets)
- Ensure that information risk assessments are reviewed at least once every quarter for all information assets where they have been assigned 'ownership' and where:
    - New systems, applications, facilities etc. is introduced that may impact the assurance of Trust Information or Information Systems.
    - Before enhancements, upgrades, and conversions associated with critical systems or applications.
- Conduct spot checks and maintain records of checks on Information Assets to ensure that all staff utilising the asset are appropriately trained and following all published guidance and protocols.

Annex D - Key Responsibilities of the Information Asset Assistants (IAA)

- Information Asset Assistants (IAA) will provide support to their IAOs to ensure that policies and procedures are followed and to recognise potential or actual security incidents. They will consult their IAOs on incident management to ensure that information asset registers are accurate and maintained up to date.

- Ensuring compliance with data sharing agreements within the local area and that information handling procedures are fit for purpose and are properly applied.

- Under the direction of their IAO, they will ensure that personal information is not unlawfully exploited and they will, upon recognising new information handling requirements (e.g. a new type of information arises) that the relevant IAO is consulted over appropriate procedures. They will consult with the IAOs regarding any potential or actual security incidents.

- Reporting to the relevant IAO on current state of local information handling and ensure that local information handling constraints (e.g. limits on who can have access to the assets) are applied, referring any difficulties to the relevant IAO. They will act as first port of call for local managers and staff seeking advice on the handling of information.

- Under the direction of their IAO, they will ensure that information is securely destroyed when there is no further requirement for it.

Annex E - Information Risk Assessment Form

Information Asset	
Information Asset Owner	
Business Unit	
Date of Assessment	

What is the threat/hazard? *(Please describe the threat/hazard of something damaging the confidentiality, integrity or availability of information)*

Examples of information asset threats may include:

***Technical risks**: loss of essential service, technical failures, unauthorised access (inadequate password management), Data loss /corruption (disc error reports, lack of patching schedule) **Physical Risks:** Physical damage to asset, Unrestricted access to office, Security of laptops/removable media, Access to printouts, **Administrative Risks**; Inappropriate use of equipment (lack of policies), lack of user training, inaccurate management information **Service Provision Risks:** Corruption /inaccuracy of patient record, Failure to update patient records*

What are the consequences? Who might be harmed and how

Examples of consequences may include:
***Financial:** Negligent use / loss of patient data (inadequate security) – up to £500,000 issued by the Information Commissioner, Fine for copyright infringement, Additional cost of re-inputting data **Reputation**: Loss of reputation arising from a loss of patient data **Staff**: Lowering of staff morale/reduced quality of service*

ASSESSMENT MATIX

Likelihood of Recurrence	Most likely consequences				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	Medium	Medium	High	Extreme	Extreme
Likely (4)	Low	Medium	Medium	High	Extreme
Possible (3)	Low	Low	Medium	High	Extreme
Unlikely (2)	Low	Low	Medium	High	High
Rare (1)	Low	Low	Medium	High	High

🟩	Low	🟨	Medium	🟧	High	🟥	Extreme

Consideration is:

What would be the potential severity (consequence of such an incident?

What is the likelihood an incident would occur given the key controls and assurances in place?

Threat/Hazard	Consequences/Who might be harmed and how.	Controls Currently in Place	Assessment	Additional Controls	Action by Whom	Action by When	Done
			in mi md mj ct ac 🟨 🟨 🟧 🟥 🟥 c 🟩 🟨 🟨 🟧 🟥 p 🟩 🟩 🟨 🟧 🟥 u 🟩 🟩 🟨 🟧 🟧 r 🟩 🟩 🟨 🟧 🟧				
			in mi md mj ct ac 🟨 🟨 🟧 🟥 🟥 c 🟩 🟨 🟨 🟧 🟥 p 🟩 🟩 🟨 🟧 🟥 u 🟩 🟩 🟨 🟧 🟧 r 🟩 🟩 🟨 🟧 🟧				

Is risk accepted?
Is risk on risk register?

If risk is not accepted, complete risk mitigation (action) plan:			
Action to reduce risk	Responsibility	Timescale	Revised risk score

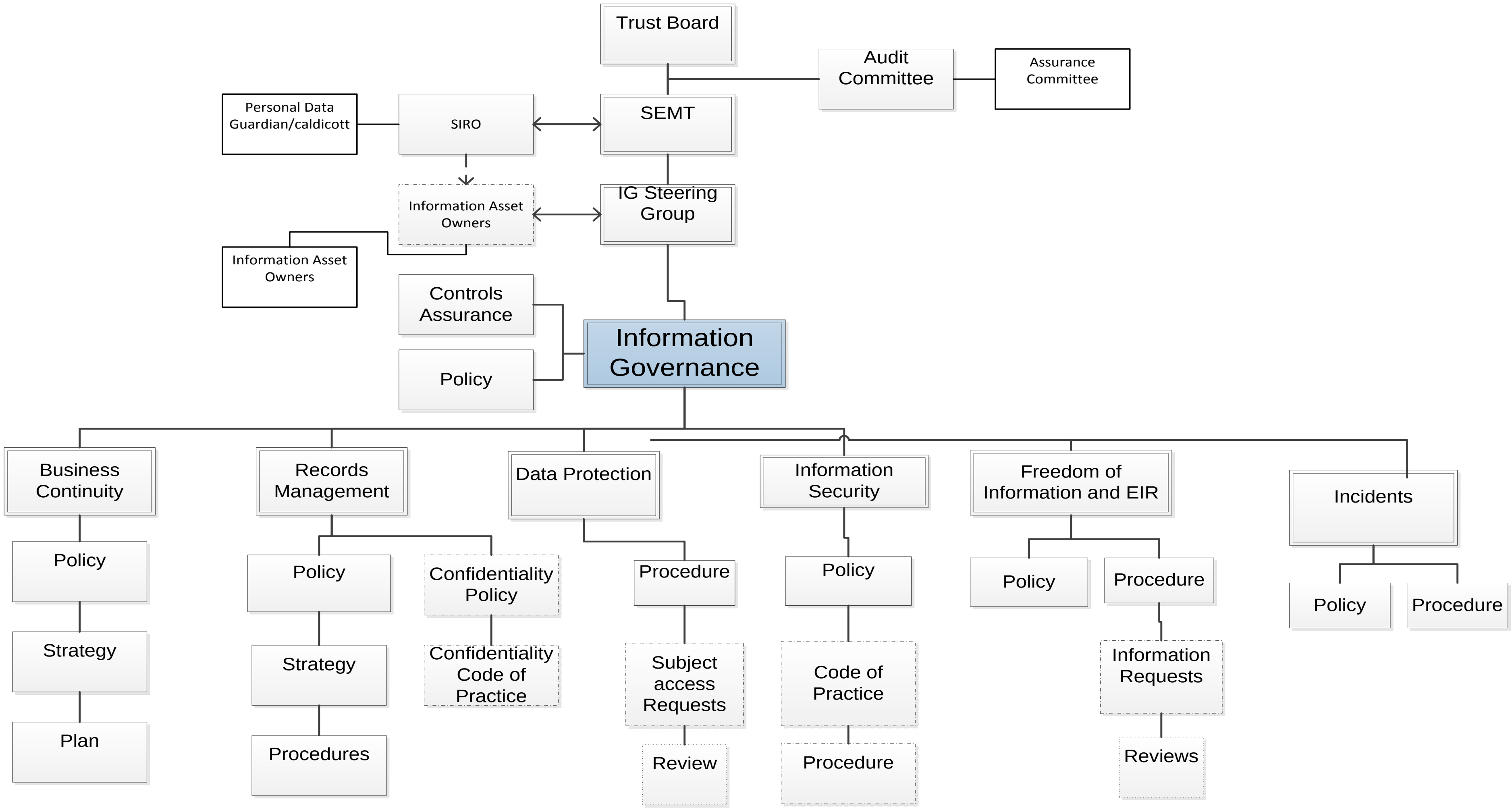
Evaluating Information Risk / Risk rating for Information Risk Assessments

A simple approach to quantifying risk is to define qualitative measures of consequences and likelihood such as the exemplars given below. This allows construction of a risk matrix which can be used as the basis of identifying acceptable and unacceptable risk. In order to prioritise actions, it is necessary to evaluate the level of risk presented by each of the identified hazards. This is done using a simple rating system (1-5). First, for each of the hazards/risks decide how likely it is to happen (Likelihood) and how serious the consequences are most likely to be (Severity) from the following guide, taking into account the measures already in place.

RISK SCORE LEVEL	ACTION AND TIMESCALE
INSIGNIFICANT Slight damage to property or equipment, Slight delay in service provision, an element of financial loss, minor clinical incident – no immediate effect on patient safety or patient care, potential breach of confidentiality where less than 5 people affected or risk assessed as low, e.g. files were encrypted.	No action is required to deal with trivial risks, and no documentary records need to be kept.
MINOR Slight damage to property or equipment, Slight delay in service provision, an element of financial loss, minor clinical incident – no immediate effect on patient safety or patient care, Loss of availability to authorised users, Serious potential breach of confidentiality e.g. unencrypted clinical records lost. Up to 20 people affected	No further preventive action is necessary, but consideration should be given to more cost-effective solutions, or improvements that impose no additional cost burden. Monitoring is required to ensure that the controls are maintained.
MODERATE Significant but temporary damage to property or equipment, failure in environmental systems (e.g. air conditioning) leaves systems unavailable, Financial loss, Temporary delay to service provision, Claim and complaint potential, Unauthorised Access to systems, Network access by unauthorised users, Serious breach of confidentiality e.g. up to 100 people affected from inadequately protected PC(s), laptop(s) and remote device(s)	Efforts should be made to reduce the risk, but the costs of prevention should be carefully measured and limited. Risk reduction measures should normally be implemented within three to six months, depending on the number of people exposed to the hazard. ***Stage 2 Assessment Required.*** Where the significant risk is associated with extremely harmful consequences, further risk assessment ***may*** be necessary to establish more precisely the likelihood of harm as a basis for determining the need for improved control measures.

	Enter the Risk on to the Risk Register if the overall score is xxx and above.
MAJOR Negative clinical outcome, Significant (permanent or long term) damage to property or equipment, Major financial loss, Long term delays in service provision, Litigation, Complaint, Media coverage, Malicious software (e.g. viruses), Serious breach of confidentiality with either particular sensitivity or up to 1000 people affected	***Stage 2 Assessment Required.*** Work should not be *started or continued* until the risk has been reduced. Considerable resources may have to be allocated to reduce the risk. Where the risk involves work in progress, the problem should normally be remedied within one to three months, depending on the number of people exposed to hazard. **Enter the Risk on to the Risk Register if the overall score is xx and above.**
CATASTROPHIC Major loss of public confidence, Permanent loss of service, equipment and property, Serious breach of confidentiality with potential for ID theft or over 1000 people affected.	***Stage 2 Assessment Required.*** Work should not be *started or continued* until the risk level has been reduced. Whilst the control measures selected should be cost-effective, legally there is an absolute duty to reduce the risk. This means that if it is not possible to reduce the risk even with unlimited resources, then the work must not be started. **Enter the Risk on to the Risk Register if the overall score is 12 and above.**

Annex F – Information Governance Policy Framework


Trust Board
Audit Committee
Assurance Committee
Personal Data Guardian/caldicott
SIRO
SEMT
Information Asset Owners
IG Steering Group
Information Asset Owners
Controls Assurance
Policy
Information Governance
Business Continuity
Policy
Strategy
Plan
Records Management
Policy
Strategy
Procedures
Confidentiality Policy
Confidentiality Code of Practice
Data Protection
Procedure
Subject access Requests
Review
Information Security
Policy
Code of Practice
Procedure
Freedom of Information and EIR
Policy
Procedure
Information Requests
Reviews
Incidents
Policy
Procedure