NHS
Wiltshire
Clinical Commissioning Group

Document information

Document type:	Framework
Document reference:	
Document title:	**Information Governance Framework**
Document operational date:	November 2015
Document sponsor:	Steve Perkins, Senior Information Risk Officer
Document manager:	Susannah Long, Governance & Risk Manager
Approving Committee/Group:	Audit & Assurance Committee (Reviewed IGG December 2017)
Approval date:	January 2018
Version:	5.0
Recommended review date:	January 2019
Intranet location:	Policies

Please be aware that this printed version of this document may NOT be the latest version. Please refer to the internet for the latest version.

Summary

This document sets out how NHS Wiltshire CCG will effectively manage Information Governance, complying with Department of Health standards and relevant legislation. The CCG aims to sustain an Information Governance culture through increasing awareness and promoting Information Governance, thus minimising the risk of breaches of personal data. The Framework is supported by additional policy documents.

Consultation

This policy was developed by South, Central and West Commissioning Support Unit Information Governance Team in consultation with the Senior Information Risk Officer, Caldicott Guardian, Lead Director for Information Governance.

Appendices

The following appendices form part of this document:

Appendix A: Useful Contacts
Appendix B: CCG IG Framework – Policies and Procedures
Appendix C: Definitions

Review Log

Version	Review Date	Reviewed By	Changes Required? (If yes, please summarise)	Changes Approved By	Approval Date
2	Aug'15	IGG	Updates to App A and App B	AAC	Nov'15
3.1	Oct'16	Senior IG Manager	Change of SIRO; Update IG Manager to Senior IG Manager.	IGG	Oct'16
4.1	Oct'17	Senior IG Manager	Change of senior role holders Addition of IAA role	IGG	Dec'17
				AAC	Jan'18

Acknowledgements

Contents

INFORMATION GOVERNANCE FRAMEWORK

1. INTRODUCTION

This document sets out the Clinical Commissioning Group (CCG) approach to Information Governance.

Robust Information Governance (IG) requires clear and effective:

- Management and leadership
- Accountability structures
- Governance processes
- Documented policies and procedures

In addition:

- Appropriately trained staff
- Adequate resources

This framework is approved by the Governing Body through the Audit and Assurance Committee and reviewed annually, or sooner should best practice or legislation require it.

This framework should be read in conjunction with the CCG's Information Governance Policy and related documents (Appendix B). There are many different standards and legislation that apply to information governance and information handling, including, though not limited to:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Caldicott Guidance
- Human Rights Act 1998
- Public Records Act 1958
- Records Management Code of Practice for Health & Social Care 2016
- Mental Capacity Act 2005
- Common Law Duty of Confidentiality
- Confidentiality NHS Code of Practice
- International information security standard: ISO/IEC 27002: 2005
- Information Security NHS Code of Practice
- NHS Information Governance Toolkit
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988

The Department of Health has developed standards of information governance requirements and compliance is measured by the Information Governance Toolkit (IGT). The CCG will submit an Information Governance Toolkit annually. The IGT covers all aspects of information governance including:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance

2. STRATEGIC AIMS

The aim of this Framework is to set out how the CCG will effectively manage Information Governance. The organisation will achieve compliance by:

- Establishing robust information governance processes that conform to Department of Health standards and comply with relevant legislation.
- Establishing, implementing and maintaining policies for the effective management of information.
- Ensuring that clear information is provided for service users, families and carers about how their personal information is recorded, handled, stored and shared.
- Ensuring that Information Governance responsibilities are included in all third party contracts and assurance is obtained with regard to the robustness of third party information governance practices during tendering and other negotiations.
- Providing clear advice and guidance to staff to ensure that they understand and apply the principles of information governance to their working practice and ensuring that information governance responsibilities are included in staff employment contracts.
- Sustaining an Information Governance culture through increasing awareness and promoting Information Governance, thus minimising the risk of breaches of personal data.
- Assessing CCG performance using the Information Governance Toolkit and Internal Audits and developing and implementing action plans to ensure continued improvement.

3. ROLES AND RESPONSIBILITIES

Accountable Officer

The Interim Chief Officer as Accountable officer of the CCG has overall accountability and responsibility for the implementation of Information Governance within the CCG and ensuring that all risks to the CCG and its partners, including those relating to information, are effectively managed and mitigated.

The Interim Chief Officer is responsible for ensuring that appropriate mechanisms are in place to support service delivery and continuity.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) should be a member of the Executive Team and is expected to understand how the strategic business goals of the CCG will be impacted by information risk. The SIRO acts as an advocate for information risk on the Governing Body and in internal discussions. The SIRO will ensure that identified information security risks are followed up and incidents managed appropriately.

The SIRO will provide guidance and leadership to the CCG's Information Asset Owners (IAOs). The Chief Financial Officer acts as SIRO for Wiltshire CCG.

Information Asset Owners (IAOs)

IAOs are directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets. In the majority of cases IAOs will be Directors, Head of Departments or equivalent.

Information asset owners (IAOs) shall ensure that information risk assessments are performed at regular intervals on all information assets where they have been assigned "ownership", following guidance from the SIRO. Mitigation plans shall include specific actions along with expected completion dates, as well as residual risks.

Information Asset Administrators (IAA)

IAOs are supported by IAAs. The role of IAA is to apply their local knowledge to assist the IAO with day-to-day management of information assets and particularly the application of records management arrangements.

Caldicott Guardian (CG)

The Caldicott Guardian (CG) is an Executive Director and senior health professional with responsibility for Corporate Governance.

The CG will act as the "conscience" of the CCG, actively supporting work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required

The CG will represent and champion confidentiality and information sharing requirements and issues at Governing Body level and, where appropriate, at a range of levels within the organisation's overall governance framework.

The CG will be supported by the CSU Senior Information Governance Manager.

The CG will be formally registered on the National Register of Caldicott Guardians. The CG for Wiltshire CCG is the Director of Nursing & Quality.

CCG Information Governance Lead

The CCG Information Governance Lead will manage the programme for Information Governance in the CCG with the support of the Commissioning Support Unit Senior Information Governance Manager and Records Manager. The CCG Information Governance Lead will report to the SIRO and manage the Information Governance Group. The CCG Information Governance Lead is the Governance & Risk Manager.

4. KEY GOVERNANCE BODIES

The following reporting structure has been implemented within NHS Wiltshire CCG in order to ensure that NHS Wiltshire CCG meets its legal and professional obligations in respect of information governance.

CCG Governing Body

The CCG Governing Body has overall responsibility for ensuring that the Organisation complies with all laws, standards, policies, codes of practice and national guidance.

Audit and Assurance Committee (AAC)

Review the establishment, maintenance and adequacy of an effective system of integrated governance, internal controls and risk management, across the whole of the organisation's activities including information governance, which supports the achievement of the organisation's objectives.

The Information Governance Group (IGG)

The Information Governance Group (IGG) is responsible for overseeing day to day information governance issues, developing and maintaining policies, standards, procedures and guidance, and promoting information governance best practice across the CCG. IGG is accountable to the CCG through the Audit and Assurance Committee.

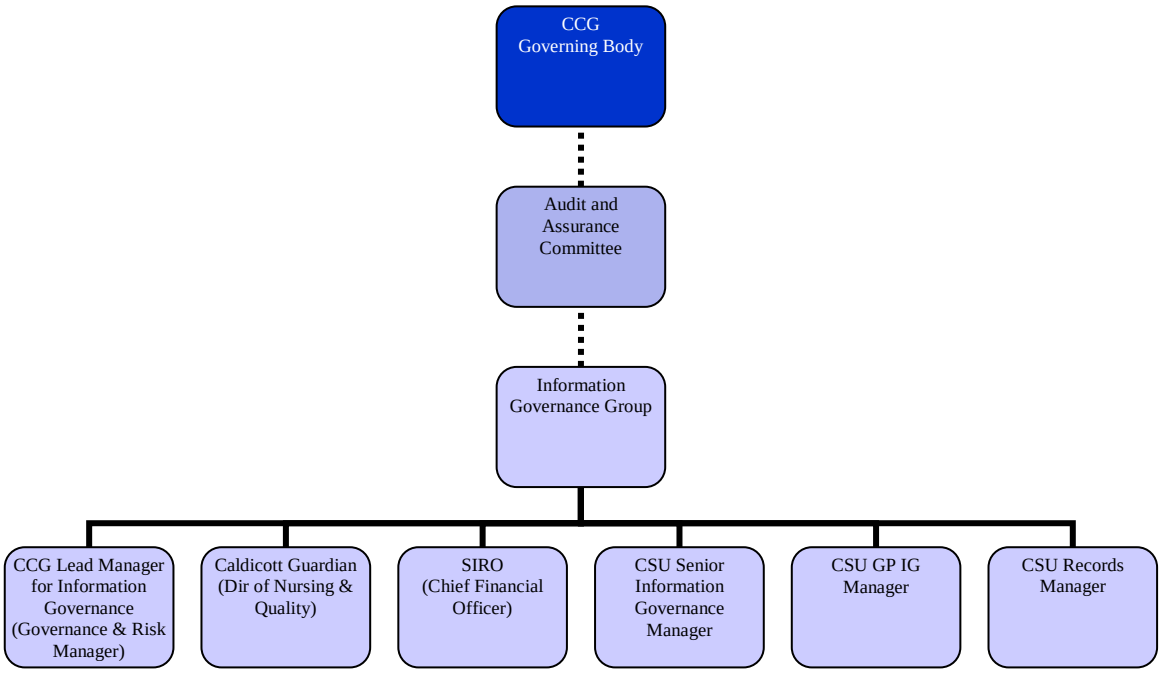


Figure 1 Key Governance Bodies/Roles

5. INFORMATION GOVERNANCE RESOURCES

Head of Information Governance
(provided by the CSU in accordance with the Corporate Services Service Specification)

The Head of Information Governance will oversee the provision of the Information Governance Service as outlined within the Central and Southern CSU Corporate Services Service Specification for Corporate Governance.

Senior Information Governance Manager
(provided by the CSU in accordance with the Corporate Services Service Specification)

The Information Governance Manager is responsible for the provision of professional advice and support to the CCG on all aspects of Information Governance, including legal and professional compliance, risk assessment and management, incident management, Information Governance Toolkit Management, document development and maintenance.

The Senior Information Governance Manager will provide support to the Caldicott Guardian as part of the Caldicott Function.

Head of FOI
(provided by the CSU in accordance with the Corporate Services Service Specification)

The Head of FOI will oversee the provision of the Freedom of Information Service as outlined within the Central and Southern CSU Corporate Services Service Specification for Corporate Governance.

Freedom of Information Team Leader
(provided by the CSU in accordance with the Corporate Services Service Specification)

The Freedom of Information Team Leader is responsible for ensuring compliance with the requirements of the Freedom of Information 2000 (“the Act”) in respect of requests received under the provisions of “the Act” and also with the development and maintenance of an approved Publication Scheme.

The Freedom of Information Team Leader is also responsible for ensuring compliance with the Subject Access Provisions of the Data Protection Act 1998 in respect of requests received from individuals (“Data Subjects”) wishing to access their own personal data (“Subject Access”).

The Freedom of Information Team Leader is responsible for ensuring compliance with the Access to Health Records Act 1990 in respect of access requests received in respect of deceased patients.

Records Manager
(provided by the CSU in accordance with the Corporate Services Service Specification)

The Records Manager is responsible for the provision of professional advice and support to the CCG on all aspects of records and information lifecycle management. This will include compliance with external requirements e.g. Records Management Codes of Practice for Freedom of Information and the NHS, provision of draft policy and procedures, training, auditing and technical support for approaches to filing e.g. file share management.

6. INFORMATION GOVERNANCE TRAINING AND AWARENESS

Training

Information Governance training is mandatory for all permanent and temporary staff. The training required is detailed in the CCG Training Needs Analysis (TNA). New members of staff will be introduced to Information Governance by their Line Manager through the Induction Checklist and Staff Handbook. The Staff Handbook will also direct the new staff member to online training available to the CCG.

All staff should complete an Information Governance on-line refresher on an annual basis.

Specialist training should be provided for the following staff:-

Senior Information Risk Owner
Information Asset Owners
Information Asset Administrators
Caldicott Guardian
CCG Lead Manager for Information Governance
Senior Information Governance Manager
Freedom of Information Team Leader
Freedom of Information Support Staff
Subject Access Support Staff

Specialist training may be made available.

Awareness

In addition to online staff training, the CCG will promote Information Governance by holding awareness sessions. Staff will be able to access the latest advice on information governance matters and review information governance responsibilities via the Information Governance intranet pages, internal communications, leaflets and posters.

Staff will be advised of the publication of new and amended policies via the staff newsletter.

7. RESPONSIBILITIES

All Managers

All Managers within the CCG are responsible for ensuring that policy and procedures are built into local processes to ensure compliance.

Managers are responsible for ensuring all staff attend/undertake mandatory awareness training.

All Staff

All staff, whether permanent, temporary, contracted or voluntary, are responsible for ensuring that they are aware of the requirements incumbent on them and for ensuring they comply with these on a day to day basis.

All staff are expected to alert their manager if they feel they need additional training or guidance and must alert the SIRO should they encounter information risks, whilst undertaking their duties.

Managers within the CCG are responsible for ensuring that the appropriate elements of this framework are built into local processes and that there is on-going compliance. This compliance will be regularly audited.

Information Security Lead
(provided by the CSU in accordance with the IT Specification)

The Information Security Lead is responsible for ensuring that Information Systems comply with Information Governance requirements.

South, Central and West Commissioning Support Unit IG Team
The IG Team within SCWCSU will act as the subject matter experts, with regards to Information Governance within the CCG.

The IG Team will be responsible for ensuring all tasks delegated to the SCWCSU meet the required standards in line with the agreed service specification.

Key tasks delegated to the SCWCSU include:-

- Developing and maintaining the currency of comprehensive and appropriate documentation that support this framework, including relevant policies and procedures.

- Ensuring that there is top level awareness and support for IG resourcing and implementation of improvements within the CCG Governing Body.

- Establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives.

- Ensuring annual assessments and audits of IG and other related policies are carried out, documented and reported.

- Ensuring that the annual assessment and improvement plans are prepared for approval by the Accountable Officer and the Governing Body in a timely manner.

- Ensuring that the approach to information handling is communicated to all staff.

- Ensuring that appropriate training is made available to staff.

- Liaising with other committees, working groups and programme boards in order to promote and integrate Information Governance standards.

- Monitoring information handling activities to ensure compliance with law and guidance.

- Providing a focal point for the resolution and/or discussion of Information Governance issues, including incident management and reporting

- Establishing, implementing and maintaining policies for the effective management of information

- Developing, implanting, monitoring and providing support for an information governance action plan to ensure that the organisation achieves the information governance standards required.

South, Central and West Commissioning Support Unit HR Manager

The Human Resources Manager is responsible for ensuring that appropriate Information Assurance clauses are included within staff employment.

APPENDIX A

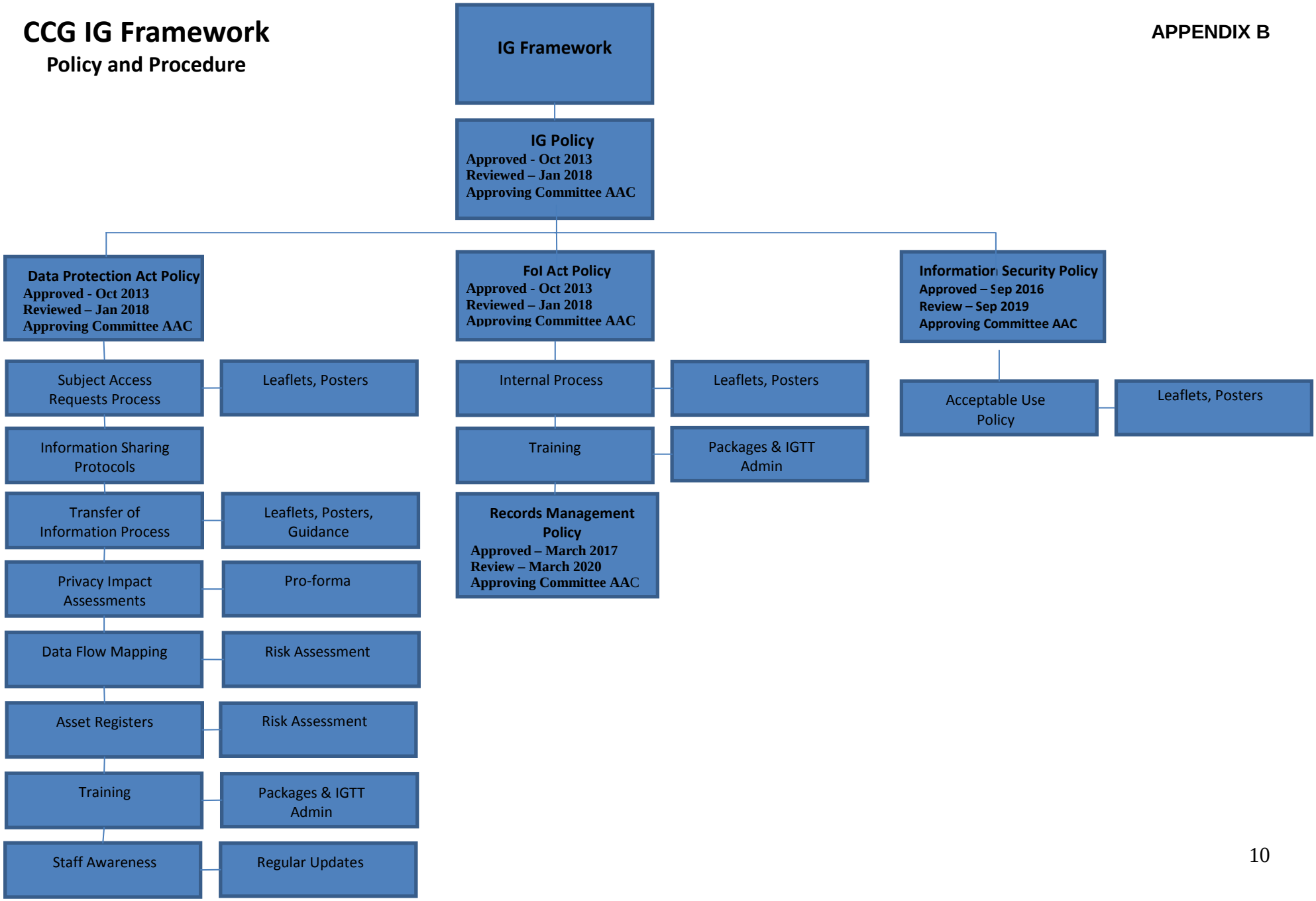
USEFUL CONTACTS

Caldicott Guardian	**Dina McAlpine** **Director of Nursing & Quality** **dina.mcalpine@nhs.net**
Senior Information Risk Owner	**Steve Perkins** **Chief Financial Officer** **steve.perkins@nhs.net**
Senior Information Governance Manager	**Barry Thorp (SCWCSU)** **barrythorp@nhs.net**
CCG Information Governance Lead	**Susannah Long** **Governance & Risk Manager** **Susannah.long@nhs.net**
Records Manager	**Rachel Lloyd (SCWCSU)** **Rachel.lloyd@nhs.net**

CCG IG Framework

Policy and Procedure

APPENDIX B



APPENDIX C

DEFINITIONS

Confidentiality

Confidentiality means ensuring that information which has been passed on with the understanding that it would be kept secret is protected. In order to be classed as confidential, the information must not be minor, it must not have already been made available to the public, unless this has been made available without the prior consent of the person or company who has passed it on. Also, there must be a reasonable chance that if the information were to be passed on to someone else, without the originator's consent, legal action could be taken. Keeping information confidential means that it must be protected from damage, so that it is available when needed, that it is kept in a format which can be accessed easily and protected from access by individuals who do not have a right to see it.

Data Protection

Data Protection means ensuring that information relating to living people is not damaged, destroyed, or stolen. That only people who have a right to, can see the information, and that the rights of the person the information relates to are complied with. Data Protection also means ensuring that only the minimum information needed for a purpose is collected and used and that information is accurate and where necessary, up to date.

Information Governance

Information Governance is a means of controlling the potential risks to the organisation, its staff, the public and others, which could result from inappropriate handling of information. Risks could include the loss or destruction of information or data, damage to information, access to information by someone who does not have a right to see it, theft of data. Examples of controls include policies and procedures, clauses in supplier and staff contracts, staff training, computer controls such as the requirement to log in to use the computer, building access controls such as toggles, and ID badges.

Information Security

Information Security is the protection of information against damage, destruction, theft and misuse and making sure that information is available and accurate.

Personal Information

Personal information means information which allows a living individual to be identified. The information on its own may allow someone to be identified, but this could also happen if it was linked with other information which is already held or may be held in the future. For example, personal information could be someone's name and address, name and GP, NHS Number and data of birth. The definition of personal information does not cover information about healthcare; this is classed as Sensitive Personal Information (see below).

Sensitive Personal Information

Sensitive personal information means information which could be damaging to someone if it became known that the information related to them. For example, sensitive personal information could be the fact that someone has heart disease, or mental illness, or that they have committed a crime, or that they are a member of a trade union. People's view of someone may be affected if they became aware of sensitive personal information which may mean that they are treated differently as a result.

Third Party Contracts

Third Party Contracts are contracts held with external companies or individuals for the provision of goods or services to the organisation.