The Queen Elizabeth Hospital King's Lynn
NHS Foundation Trust

INFORMATION GOVERNANCE POLICY

Primary Intranet Location	Version Number	Next Review Year	Next Review Month
Information Management & Governance	8.0	2021	January

Current Author	Phil Cottis
Author's Job Title	Head Health Records & IG
Department	IM&T
Ratifying Committee	Information Governance Committee
Ratified Date	8th January 2018
Owner	Jon Wade
Owner's Job Title	Director of Strategy & IT Services

It is the responsibility of the staff member accessing this document to ensure that they are always reading the most up to date version. This will always be the version on the intranet

Related Policies	Confidentiality Code of Conduct Data Protection Policy Freedom of Information Policy Information Governance Management Framework Information Governance Strategy Information Lifecycle & Records Management Policy Information Security Policy Information Sharing Policy

Stakeholders	Information Governance Committee

Version	Date	Author	Author's Job Title	Changes
V3	December 2010	Nic McCullagh	Information Governance Manager	Annual review
V4	February 2012	Phil Cottis	Head of Health Records & Information Governance	Annual review
V5	December 2012	Phil Cottis	Head of Health Records & Information Governance	Annual review and format change
V6	November 2013	Phil Cottis	Head of Health Records & Information Governance	Annual review
V7	November 2014	Phil Cottis	Head of Health Records & Information Governance	Annual review
V7.1	June 2016	Phil Cottis	Head of Health Records & Information Governance	Amendments to Section 3 'Responsibilities'
V8	January 2018	Phil Cottis	Head of Health Records & IG	No material changes

Summary of the policy
The purpose of this policy is to provide details of the framework for implementation of the Information Governance (IG) strategy to enable the Trust to meet its responsibilities for the management of information assets and resources.

Key words to assist the search engine
Caldicott, Confidentiality, Information, Information Governance, Security, Sharing.

CONTENTS

INFORMATION GOVERNANCE POLICY

1 INTRODUCTION

1.1 Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. It provides a consistent way for employees to deal with the many different information handling requirements including:

- Information Governance Management;
- Confidentiality and Data Protection Assurance;
- Information Security Assurance;
- Clinical Information Assurance for Safe Patient Care;
- Secondary Use Assurance; and
- Corporate Information Assurance.

1.2 It is of paramount importance to ensure that information is effectively and efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

1.3 The policy is intended to be fully consistent and compatible with the policies and practices throughout the NHS and the Trust strategy for Information Governance and is developed to achieve compliance to the Care Quality Commission Outcomes.

2 PURPOSE

2.1 The purpose of this policy is to provide details of the framework for implementation of the Information Governance (IG) strategy to enable the Trust to meet its responsibilities for the management of information assets and resources.

2.2 The aims of this document are:

2.2.1 To maximise the value of organisational assets by ensuring that data is:

- Held securely and confidentially.
- Obtained fairly and lawfully.
- Recorded accurately and reliably.
- Used effectively and ethically, and
- Shared and disclosed appropriately and lawfully.

2.2.2 To protect the Trust's information assets from all threats, whether internal or external, deliberate or accidental. The Trust will ensure that:

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Information will be supported by the highest quality data.

- Regulatory and legislative requirements will be met.
- Business continuity plans will be produced, maintained and tested.
- Information security training will be available to all staff, and
- All breaches of information security, actual or suspected, will be reported to, and investigated by the Head of Health Records & Information Governance.

2.3 This policy applies to:

- All information used by the Trust;
- All information systems managed by the Trust;
- Any individual using information 'owned' by the Trust; and
- Any individual requiring access to information 'owned' by the Trust.

3 DEFINITIONS

3.1 **Breach of Confidentiality**
A breach of confidentiality is the unauthorized disclosure of personal information provided in confidence.

3.2 **Confidential Information**
Confidential information can be anything that relates to patients, staff or any other information (such as contracts, tenders etc) held in any form (such as paper or other forms like electronic, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer or on portable devices such as laptops, PDAs, BlackBerrys, mobile telephones and USBs) or even passed by word of mouth.

3.3 **Corporate Information**
Corporate information refers to information generated by the Trust, other than clinical or patient information and describes the records generated by an organisation's business activities.

3.4 **Disclosure**
This is the divulging or provision of access to data.

3.5 **Information**
Information is a corporate asset. Whilst all records are information, not all information is a record.

3.6 **Personal Confidential Data**
Personal confidential data is information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

3.7 **Public Interest**
Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.

3.8 **Sensitive Data**

Data held about an individual which contains both personal and sensitive information. There are only seven types of information detailed in the Data Protection Act 1998 that are deemed as sensitive:

- Racial or ethnic origin;
- Religious or other beliefs;
- Political opinions;
- Trade union membership;
- Physical or mental health;
- Sexual life; and
- Criminal proceedings or convictions.

4 RESPONSIBILITIES

4.1 **Chief Executive**

The Chief Executive has overall responsibility the establishment of policy governing access to, and the use of personal confidential data and where appropriate, the transfer of that information across organisational boundaries. As accounting officer the Chief Executive is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Maintaining confidentiality is pivotal to the Trust being able to supply a first class confidential service that provides the highest quality patient care. The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

4.2 **Senior Information Risk Owner**

An Executive Director has been appointed as the Senior Information Risk Owner (SIRO) with overall responsibility for information governance, of which confidentiality is a key part.

4.3 **Caldicott Guardian**

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The Caldicott Guardian is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

4.4 **Information Governance Committee**

The Information Governance Committee is responsible for ensuring that this policy is implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Board assurance in this respect. See Appendix 2 for the IG Committee's Terms of Reference.

4.5 **Head of Health Records & Information Governance**

The Head of Health Records & Information Governance is responsible for maintaining the currency of this policy, providing advice on request to any member of staff on the issues covered within it, and ensuring that training is provided for all staff groups to further their understanding of the principles and their application.

4.6 **Senior Managers**

Senior Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going

compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon via the Incident Reporting Procedure.

4.7 **All Staff**

Staff working in or on behalf of the Trust (this includes contractors, temporary staff, secondees and all permanent employees) must adhere to this policy to support the reputation of the Trust and where relevant of their profession. Everyone has a duty to respect a data subjects rights to confidentiality.

4.8 **Volunteers**

Although not directly employed by the Trust, all Volunteers are bound by the same requirements for confidentiality as paid staff. Volunteers will be required to:

- Sign a Confidentiality Agreement;
- Undertake Trust Core Induction which includes an 'Introduction to Information Governance' session; and
- Complete an annual Information Governance training course. Those Volunteers with access to personal confidential data (eg patient, staff or fellow volunteers) will be required to complete the Information Governance Workbook, and pass the assessment, annually.

5 INFORMATION GOVERNANCE PRINCIPLES

5.1 The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

5.2 The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

5.3 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 staff to ensure and promote the quality of information and to actively use information in decision making processes.

6 INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK

6.1 The Trust has developed a framework for its Information Governance Policy. This is supported by a set of Information Governance policies and related procedures to cover all aspects of Information Governance which are aligned with the NHS Operating Framework and the Information Governance Toolkit requirements.

6.2 The Key Information Governance Policies are:

Policies	***Summary***
Data Protection Policy	*This policy sets out the roles and responsibilities for compliance with the*

	Data Protection Act.
Freedom of Information Policy	*This policy sets out the roles and responsibilities for compliance with the Freedom of Information Act and Environmental Information Regulations.*
Confidentiality Code of Conduct	*This policy lays down the principles that must be observed by all who work within the Trust and have access to personal or confidential business information. All staff must be aware of their responsibilities for safeguarding confidentiality and preserving information security in order to comply with common law obligations of confidentiality and the NHS Confidentiality Code of Practice.*
Information Security Policy	*This policy is to protect, to a consistently high standard, all information assets. The policy defines security measures applied through technology and encompasses the expected behaviour of those who manage information within the organisation*
Information Lifecycle & Records Management Policy	*This policy is to promote the effective management and use of information, recognising its value and importance as a resource for the delivery of corporate and service objectives.*
Information Sharing Policy	*The policy will ensure that all information held or processed by the Trust is made available subject to appropriate protection of confidentiality and in line with the terms and conditions under which the data has been shared with the Trust. This policy sets out what is required to ensure that fair and equal access to information can be provided and is supported by a range of procedures.*

6.3 An Information Governance Management Framework has been produced which lists all the IG related Trusts policies and procedures. These documents are published and implemented in accordance with the 'Policy For the Development and Management of Procedural Documents'. The monitoring of compliance with the policies and review of the policies is undertaken in accordance with the monitoring and review statements in each policy.

6.4 An Information Governance Staff Guide has been developed to provide an introduction to Information Governance and summarises the key user obligations that support the Trust's Information Governance policies.

7 MAIN THEMES

7.1 There are six key interlinked strands to the Information Governance Policy:

- Openness;
- Legal Compliance;
- Information Security;
- Information Quality Assurance;
- Records Management; and
- Information Governance Training.

7.2 Openness

- Non-confidential information about the Trust and its services will be available to the public through a variety of media;
- The Trust has established and will maintain policies to ensure compliance with the Freedom of Information Act;
- The Trust undertakes or commissions annual assessments and audits of its freedom of information policies and arrangements;
- Patients have ready access to information relating to their own health care, their options for treatment and their rights as patients;
- The Trust has clear procedures and arrangements for liaison with the press and broadcasting media; and
- The Trust has clear procedures and arrangements for handling queries from patients and the public.

7.3 Legal Compliance

- The Trust regards all personal confidential data relating to patients as confidential;
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements;
- The Trust regards all personal confidential data relating to staff as confidential except where national policy on accountability and openness requires otherwise;
- The Trust has established and will maintain policies to ensure compliance with the Data Protection Act, Human Rights Act, the common law duty of confidence and the Confidentiality NHS Code of Practice;
- The Trust has established and will maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act); and
- The Information Governance legal compliance requirements are linked to the Trust's disciplinary procedures as appropriate.

7.4 **Information Security**

- The Trust has appointed a Senior Information Risk Officer (SIRO) at Board level;
- The Trust has established and will maintain standards and policies for the effective and secure use and management of its information assets and resources;
- The Trust has established and will maintain standards and guidance for the effective and secure transfer of information into and out of the Trust;
- The Trust has established and will maintain standards and policies for the disclosure of information;
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements;
- The Trust promotes effective confidentiality and security practice to its staff through policies, procedures and training; and
- The Trust has established and will maintain incident reporting procedures and monitors and investigates all reported instances of actual or potential breaches of confidentiality and security.

7.5 **Information Quality Assurance**

- The Trust will establish and maintain policies and procedures for information quality assurance;
- The Trust will undertake or commission annual assessments and audits of its information quality;
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services;
- Wherever possible, information quality should be assured at the point of collection;
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards; and
- The Trust will promote information quality through policies, procedures/ user manuals and training.

7.6 **Records Management**

- The Trust has established and will maintain policies and procedures for the effective management of records;
- The Trust will undertake or commission annual assessments and audits of its records management;
- Managers are expected to ensure effective records management within their service areas;
- The Trust promotes records management through policies, procedures and training; and
- The Trust uses Records Management: NHS Code of Practice (Part 1 2006; Part 2 revised 2009) as its standard for records management.

7.7 **Information Governance Training**

- The Trust has established and will maintain the Information Governance Training

Programme for the effective delivery of Information Governance training, awareness and education;

- The Trust provides Information Governance induction training directed at all new members of staff;
- The Trust mandates annual mandatory Information Governance training and requires all staff to pass a comprehension assessment;
- The Trust provides general Information Governance awareness on a regular basis through newsletters, articles, team meetings etc; and
- Evaluation of Information Governance training is undertaken to assess the effectiveness of the training and influence changes to future training.

8 ESCALATION

8.1 Any breach of this policy could result in a member of staff facing disciplinary action. A copy of the Trust Disciplinary Policy and Procedure is available from the Human Resources Department or on the Trust Intranet.

9 TRAINING

9.1 Support to implement this policy will be provided by mandatory annual IG Training delivered by the IG Team, IG Workbooks and the online IG Training Tool.

10 DISSEMINATION OF DOCUMENT

10.1 Following approval by the Information Governance Committee, this policy will be uploaded onto the Trust intranet site under 'Information Management & Governance' and on the Information Governance intranet page. Notification will be through a broadcast email and through the IG & RA Newsletter.

11 REFERENCES

11.1 References to Standards

- Information Governance Toolkit v.14.1

11.2 Legislation

- Abortion Regulations 1991 and subsequent amendments
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Data Protection Act 1998
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Health and Social Care Act 2008
- Human Fertilisation and Embryology Act 1990
- Human Rights Act 1998
- Mental Capacity Act 2005

- NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
- Re-use of Public Sector Information Regulations 2005

11.3 **Guidance**

- Caldicott Guardian Manual 2010
- Caldicott Reports 1997 & 2013
- Care Quality Commission / Monitor
- Care Record Guarantee 2009
- Confidentiality: NHS Code of Practice 2003
- Health Service Circular 1999/012
- Information Security Management: NHS Code of Practice 2007
- NHS Information Governance: Guidance on Legal and Professional Obligations 2007
- NHS Litigation Agency Risk Management Standards
- Records Management: NHS Code of Practice - Part 1 2006, Part 2 2009

12 EQUALITY IMPACT STATEMENT

12.1 A Stage 1 (Screening) - Equality Impact Assessment has been undertaken and no negative impact on any group was indicated (see Appendix 1).

13 MONITORING COMPLIANCE

13.1 Compliance with this policy will be monitored in the following manner (see table below):

Key elements (Minimum Requirements)	Process for Monitoring (e.g. audit)	By Whom (Individual / group /committee)	Frequency of monitoring
Roles and responsibilities	Monitored at appraisal, following review of the individual's knowledge & skills framework (KSF) together with the job description.	Line manager	Annually
How the organisation provides IG Training. In house training sessions are delivered regularly throughout the year to meet the needs of the Trust	Electronic Staff Record (ESR) is utilised to identify all staff who are non- compliant	IG Team	Monthly
Reducing the number of Information Governance breaches	Management of incidents relating to Information Governance	IG Team	Monthly

Ensuring best practice across the Trust	Undertaking Confidentiality Audits	IG Team	Monthly

APPENDIX 1

EQUALITY IMPACT ASSESSMENT
Equality Impact Assessment Tool
(To be completed and attached to any policy document when submitted to the appropriate committee for ratification.)

STAGE 1 - SCREENING

Name & Job Title of Assessor: Phil Cottis – IG & RA Manager	**Date of Initial Screening: 01/12/09**
Policy or Function to be assessed: Information Governance Policy	

		Yes/No	**Comments**
1.	**Does the policy, function, service or project affect one group more or less favourably than another on the basis of:**		
	• Race & Ethnic background	No	
	• Gender including transgender	No	
	• Disability:- This will include consideration in terms of impact to persons with learning disabilities, autism or on individuals who may have a cognitive impairment or lack capacity to make decisions about their care	No	
	• Religion or belief	No	
	• Sexual orientation	No	
	• Age	No	
2.	**Does the public have a perception/concern regarding the potential for discrimination?**	No	

If the answer to any of the questions above is yes, please complete a full Stage 2 Equality Impact Assessment.

Signature of Assessor: Phil Cottis **Date: 08/01/2018**

Signature of Line Manager: Jon Wade **Date: 08/01/2018**

APPENDIX 2: IG COMMITTEE TERMS OF REFERENCE

Definitions and Scope

Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. It provides a consistent way for employees to deal with the many different information handling requirements including:

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

Overall Purpose

The Information Governance Committee is a standing committee accountable to the Trust Board. Its purpose is to support and drive the broader Information Governance agenda and provide the Board with the assurance that effective Information Governance best practice mechanisms are in place within the organisation and to oversee the implementation of those areas of work that sit within the Information Governance framework.

Responsibilities

- To ensure that an appropriate comprehensive Information Governance (IG) framework and systems are in place throughout the organisation in line with national standards;
- To undertake an annual baseline assessment and performance update of the IG work areas using the Department of Health IG Toolkit;
- To prepare the annual final submission against the IG Toolkit, and to report this to the Board;
- To evaluate and review the implementation of relevant strategies, policies, procedures and action plans including raising staff awareness of them;
- To drive those activities which will secure compliance with the regulatory framework;
- To develop and implement an annual action plan for the IG work areas ie: Information Governance Management, Confidentiality and Data Protection Assurance, Information Security Assurance, Clinical Information Assurance, Secondary Use Assurance and Corporate Information Assurance;
- To use the action plan as a means of performance managing the IG work throughout the year;

- To ensure there are clear lines of authority and accountability for members of staff leading the implementation of the discrete areas of work in the action plan;
- To receive regular progress reports from members of staff leading a discrete area of work;
- To approve contingency plans where progress has deviated from the plan;
- To monitor the organisation's clinical and corporate information handling activities to ensure compliance with law and guidance;
- To oversee the monitoring and audit of working practices and clinical and corporate record keeping standards to verify accuracy, accessibility, integrity and validity and propose corrective action where necessary;
- To monitor and review untoward occurrences and incidents relating to IG and ensure that effective remedial and preventative action is taken. Serious Incidents (SIs) concerning information risk will be reported to the SIRO, and then reported to the Trust Board;
- To drive the IG training agenda via implementation of the IG Training Programme, ensuring the Trust's approach to information handling is communicated to all staff;
- To develop and maintain the Trust's Publication Scheme; and
- To provide a focal point for the resolution and / or discussion of IG issues.

Reporting Committees / Groups
- Health Records Management Committee;
- Data Quality & Access Working Group;
- Registration Authority Working Group;
- IG Mandatory Training Working Group; and
- IG Toolkit action plan working groups as appropriate.

Accountability
- Clinical Governance Committee;
- Quality Committee;

- Extended Management Team; and
- IT Strategic Programme.

Chair / Deputy Chair
- Chair – Director of Strategy & IT Services / Senior Information Risk Owner;
- Deputy Chair – Caldicott Guardian.

Membership
- Director of Strategy and IT Services / Senior Information Risk Owner;
- Caldicott Guardian;
- Head of Health Records & IG;
- Information Governance & RA Officer;
- Company Secretary;
- Complaints Manager;
- Head of Communication;
- Head of ICT;
- Head of Business Support;
- Head of Integrated Clinical Governance;
- Head of Facilities (Hotel Services);
- Human Resources & Organisational Development representative;
- Voluntary Services Manager
- Divisional representative;
- Clinical representative;
- Nursing representative;
- Legal Services Manager; and
- Others – *by invitation depending on the agenda items and current projects*

Deputies should be sent to meetings

Quorum
A quorum shall be 6 members, including the Chair or Deputy Chair.

Frequency
Bi-Monthly - additional meetings to be convened if required.

Minutes
Formal minutes will be kept of the proceedings and submitted for approval at the next meeting.