Basildon and Thurrock University Hospitals NHS
NHS Foundation Trust

Document Title:	**INFORMATION GOVERNANCE POLICY**
Document Purpose:	This policy has been produced to provide an overview of all Information Governance requirements and ensure that all staff are aware of relevant legislation, NHS guidance and their individual responsibilities
Document Statement:	Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.
Document Application:	Organisation wide
Responsibilities for Implementation:	Information Governance Group, General Managers.

Main imperatives of the policy:
To ensure:

- Compliance with all legislation, guidance and standards relating to Information Governance
- That individuals are aware of their responsibilities for Information Governance
- The Trust develops and maintains the required standards of Information necessary for Foundation Trust
- The balance between integrity, availability and confidentiality of personal information is maintained
- All reasonable organisational and technical measures are taken to ensure that the personal information held by the Trust is kept secure and used only for fair and lawful purposes.
- All individuals, for whom data are processed, are informed of the purpose of that processing, how their records will be kept secure and what disclosures may occur.
- That the transfer and sharing of personal information is strictly controlled and that data is anonymised wherever possible.
- Openness in relation to non-confidential information in line with responsibilities under the Freedom of Information Act 2000.

Document Classification:	Information Management	**Document Reference:**	IM/PO/00011
Version Number:	7	**Effective Date:**	March 2005
Issued by:	Information Governance Manager	**Review Date:**	October 2014
Author:	Health Records Service Manager	**Expiry Date:**	October 2022
Sponsor:	Director of Nursing		

Associated Documents:
Information Governance Policy Framework
Information Governance Strategy
Information Security Policy
Procedures for Transferring Information & Use of Portable Devices
Risk Management Strategy
Health Records Policy
Freedom of Information Act Policy
SI Management Procedure

APPROVAL RECORD

Validated by Facilitator:	Patient Safety Team/ Document Control Group	**Date:** September 2012
Agreed by Specialist Group:	Information Governance Group	**Date:** August 2012

DOCUMENT HISTORY

REVISION HISTORY

Revision Date	Previous Revision date	Summary of Changes	Changes marked
October 2010	March 2010	Changes to IGG responsibilities to reflect NHS Operating Framework	
October 2010	March 2010	Minor change to SIRO role regarding Statement of Internal Control	
October 2010	March 2010	Changes to staff training to reflect the mandated IGTT in the NHS Operating Framework	
October 2010	March 2010	Added sections on Consultation, Approval, Ratification, Dissemination, Implementation, Review, Revision Arrangements and Document Control.	
October 2010	March 2010	Changes to IG Policy Framework	
October 2010	March 2010	Changes to Confidentiality Code of Conduct for Staff	
September 2011	October 2010	Changes to job title (Information Security Facilitator changed to Information Governance Manager)	
September 2011	October 2010	Removal of references to Head of Health Records & Information Governance	
September 2011	October 2010	3.9 – Inclusion of paragraph relating to BS10008:2008 for EMR	
September 2011	October 2010	Review of document changed from annually to 3 yearly (or sooner if legislation or national guidance changes)	
July 2012	September 2011	Section 6.3 (Training) changed from using CfH official website to Trust NLMS/MOODLE training systems	

CONTENTS

1. INTRODUCTION

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures and management accountability structures provide a robust governance framework for Information management.

This high level policy is underpinned by, and must be read in conjunction with, specific detailed policies and procedures relating to each element of Information Governance. A list of relevant Trust policies is provided in Appendix A.

1.1 Standards

Standards have been set by the Department of Health and these have been developed into the Information Governance Toolkit. All NHS organisations are required to assess their performance against these standards on an annual basis. Results of these assessments will form part of the Trust's performance monitoring and will impact on the Statement of Internal Control. The toolkit standards are based upon the HORUS model in order to ensure that information is:

- **H**eld securely and confidentially
- **O**btained fairly and lawfully
- **R**ecorded accurately and reliably
- **U**sed effectively and ethically
- **S**hared appropriately and lawfully

1.2 Scope

Information Governance covers a wide range of legislation and NHS Guidance relating to the processing of information and are grouped into the following initiatives:

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

1.3 The Benefits of the Information Governance Framework

- 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 and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards.

- To enable organisations to understand their own performance and manage improvement in a systematic and effective way.

2. ROLES AND RESPONSIBILITIES

2.1 All Staff

Every employee, which includes permanent, temporary, locums, contractors, voluntary, work experience and bank staff, has a legal, moral and contractual obligation for maintaining Information Governance, regardless of their position, standing or level of knowledge.

2.2 Information Governance Group

The Group is responsible for the implementation of Information Governance standards across the Trust and for monitoring performance against these standards and addressing areas of non-compliance ensuring that improvements plans are put in place. The Group is responsible for overseeing the work required for the Connecting for Health Information Governance Toolkit annual assessment, which includes meeting the national expectations clearly defined within the NHS Operating Framework (Informatics Planning Guidance):

- Continuing to demonstrate compliance with the key IG standards through the achievement of at least level 2 performance in terms of the NHS IG Toolkit and ensuring plans are in place to progress beyond this minimum where it has been achieved;
- Ensuring an IG audit utilising the centrally provided audit methodology is included within each organisation's auditors work plan.

The following key individuals are members of the Information Governance Group:

2.2.1 Caldicott Guardian

The Director of Nursing is the Trust's Caldicott Guardian and has the following Trust responsibilities:

- To ensure that all routine uses of person-identifiable patient information are identified, documented and justified.
- To oversee the process for dealing with ad hoc requests for person-identifiable patient information for non-clinical purposes.
- To ensure standard procedures and protocols are in place to govern access to person-identifiable patient information.
- To ensure protocols for releasing information for research and audit are in line with applicable information governance standards.
- To work with other care providers and linked agencies to facilitate better sharing of relevant information about patients, in a manner that facilitates joined-up care across institutional boundaries while ensuring that patients' legal rights and the Caldicott Principles are maintained.

2.2.2 Senior Information Risk Officer

The Director of Strategic Development is the Senior Information Risk Officer and has the following Trust responsibilities:

- To act as an advocate for information risk on the Board and in internal discussions.
- To take ownership of the risk assessment processes for information risk including the review of the annual information risk assessment to support and inform the Statement of Internal Control.
- To provide written advice to the Accounting Officer (Chief Executive) on the content of the Statement on Internal Control with regard to information risk (including details of any data loss and confidentiality breach incidents) for inclusion in the Annual Report.

- To review and agree actions in respect of identified information risk.
- 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 ensure that the Board is adequately briefed on information risk issues.

2.2.3 Information Governance Manager

The Trust's Information Governance Manager is responsible for:

- Overseeing implementation of and compliance with the 8 Data Protection Principles
- Investigating any information security incidents, risk or breaches and ensuring appropriate action is taken.
- Ensuring notification to the Information Commissioner, of all relevant information processes, is up to date at all times
- Co-ordinating the provision of information security training to all staff
- Providing advice and support on non-technical aspects of information security.
- Ensuring the Information Governance Policy Framework and Information Governance Accountability Arrangements are reviewed and up-to-date
- The co-ordination of the annual Department of Health Information Governance Assessments
- To co-ordinate Information Security Workplace Assessments

2.2.4 Assistant Director of IT

The Assistant Director of IT, supported by the IT Project Manager, have the role of IT Security Lead and they are responsible for:

- Ensuring all Trust requirements and relevant legislation for IT is adhered to
- Ensuring systems and processes are in place to minimise the risk of security breaches
- Undertaking audits of all IT systems
- Providing advice and support on technical issues surrounding Information Governance.

2.2.5 Corporate Secretary

The Corporate Secretary is also head of the Trust's Compliance Unit and is responsible for Corporate Information Assurance which includes ensuring:

- That the Trust has a carried out an audit of all its corporate records and information and has a comprehensive understanding of the corporate information it holds.
- That the Trust has documented and implemented procedures that specify how electronic corporate records are to be created, including referencing, version control, naming, filing and filing structures, and applying appropriate protective marking. All staff members that create electronic corporate records comply with the procedures.
- That the Trust has documented and implemented procedures that specify how paper corporate records are to be created and tracked/traced, including guidance on referencing, version control, naming, filing, indexing and applying appropriate protective marking. All relevant staff members comply with the procedures.
- That an Information Lifecycle Policy and Implementation Strategy are in place and regularly reviewed and updated.

2.2.6 Freedom of Information Lead

The Communication Manager is the Trust's Freedom of Information lead and is responsible for:

- Ensuring the Trust's publication scheme is up to date and available
- Ensuring that requests made under the Freedom of Information Act 2000 are responded to within the given timescales
- That the Trust has publicly available, documented and implemented procedures for FOI Act compliance with clear responsibility for responding to information requests by effectively informed and resourced staff. All staff are effectively informed of the need to support FOI requests. The procedures are reviewed regularly, and there are additional procedures to assess performance in meeting the statutory timeframes and applicant satisfaction with the process.

2.2.7 PAS & Data Quality Manager

The Head of Information Management, supported by the PAS & Data Quality Manager has responsibility for Information Quality Assurance across the Trust and for ensuring:

- Information is of the highest quality in terms of accuracy, timeliness and relevance.
- Data quality standards are monitored on a regular basis for the purposes of identifying areas where improvement is required, ensuring that responsibility is taken for co-ordinating actions required to resolve these issues.
- Information returns to the Department of Health and Department of Health and Social Care and other external bodies are completed and despatched in a timely and efficient manner.

2.3 Departmental Managers

- Ensuring that Information Governance measures are upheld within their department
- Advising all staff of their security and confidentiality responsibilities
- Determining required access levels to specific computer systems ensuring no unauthorised access
- Ensuring that adequate training is provided to all staff
- Implementing procedures to minimise the risk of fraud / theft / disruption of their systems.
- Ensuring current documentation is maintained for all critical job functions.
- Supporting planned audits of Information Governance and any resulting actions
- Investigating any security issues raised by members of staff, patients or visitors

2.4 Information Asset Owners

- Ensuring continued security of their systems,
- Complying with and enforcing relevant legislation and Information Governance standards on and by users of their system
- Ensuring that contingency documentation exists for their system and this is reviewed updated and tested on a regular basis.

2.5 Information Security Leads

Each Directorate has an Information Security Lead who is responsible for:

- Co-ordinating actions required by the Trust to maintain and improve Information Governance
- Actively working to improve standards within their Directorate
- Encouraging staff within their departments to raise matters of concern
- Ensuring that all staff in their departments are aware of this policy

2.6 Third Parties

Contracts for any third party individual or company, required to carry out work for the Trust must contain Data Protection and Freedom of Information clauses if working within patient areas, with Trust systems or have access to confidential information. Contracts where this does not occur are required to sign a Data Security and Confidentiality Undertaking (DSCU). For further information contact the Information Governance Manager on ext 1957

3. RELEVANT LEGISLATION / GUIDANCE

This section is a summary only of key legislation and NHS Guidance relating to Information Governance. Further information sources are provided in Appendix A.

3.1 Data Protection Act 1998 (replacing the 1984 Act)

The purpose of the Act is to safeguard the fundamental rights of individuals and to protect them with regard to processing personal data about them. Under the new Act the requirements have now extended to manual records and the rights of individuals have increased significantly, including the right to access personal information held about them. The Act contains 8 main principles governing the processing of personal data:

- 1st Principle: ‘Personal data shall be processed fairly and lawfully’
- 2nd Principle: ‘Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes’.
- 3rd Principle: ‘Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed’.
- 4th Principle: ‘Personal data shall be accurate and, where necessary, kept up to date’
- 5th Principle: ‘Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose(s)’.
- 6th Principle: ‘Personal Data must be processed in accordance with the Data Subjects Rights’
- 7th Principle states ‘Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.’
- 8th Principle: ‘Personal Data may not be transferred to a territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to processing of personal data’.

The Act imposes strict regulations and it is important that these principles are adhered to at all times. Staff must be fully aware of how patient information is processed across the Trust, and of the procedures for providing access to information in order to respond to patient enquiries. Further information on Data Protection can be found in the Trust’s Information Security Policy.

3.2 Access to Health Records Act 1990

Under the Data Protection Act 1998 individuals (patients and staff) have the fundamental right to have access to personal records held about them. Access to medical records was previously covered by the Access to Health Records Act 1990, but this Act now only covers any requests made for access to health records relating to deceased patients. All others requests are dealt with under the requirements of the Data Protection Act. Further information on Access to Health Records can be found in the Trust's Health Records Policy

3.3 Freedom of Information Act 2000

The Freedom of Information Act came into fully into force in January 2005 and creates a statutory right for an individual to know whether a public authority holds specified corporate information, and, if it does, to have that information communicated. Whereas the Data Protection Act 1998 deals with the rights of individuals regarding their own personal information, The Freedom of Information Act covers corporate information. The Act also requires public authorities to release information pro-actively through approved publication schemes. In order for the authority to locate the information requests from individuals must be clear and in writing. The Trust has a responsibility to respond to requests within 20 days of receipt. There are some exemptions to the Act, including personal information that is covered by the Data Protection Act.

3.4 The Caldicott Report

The Caldicott Report was published in December 1997 following a review of all information flows involving patient-identifiable data. The report outlines eighteen recommendations for ensuring patient confidentiality is maintained when using or sharing patient identifiable data. The Trust is committed to implementing these recommendations, one of which was to appoint a 'Caldicott Guardian' to oversee patient confidentiality within the Trust as described in the section on "Responsibilities". The general principles of the Caldicott report can be summarised as follows:

1. Justify the purpose for use of patient identifiable information
2. Do not use patient identifiable information unless absolutely necessary
3. Use the minimum necessary patient identifiable information
4. Access to patient identifiable information should be on a strict need to know basis
5. Everyone with access to patient identifiable information should be aware of their responsibilities
6. Understand and comply with the law

All staff are responsible for ensuring patients rights to confidentiality are maintained at all times and ensuring that they have complied with the above principles. For further information please refer to the Policy for Sharing of Personal Information.

3.5 DH Information Security Management Code of Practice

The Information Security Management Code of Practice, published by the Department of Health, is a guide to the methods and required standards of practice in the management of information security within the NHS. Its purpose is to identify and address security management in the processing and use of NHS information and is based on current legal requirements, relevant standards and professional best practice.

3.6 DH Records Management Code of Practice

Under the requirements of DH Records Management Code of Practice, which was published in April 2006 to replace HSC 1999/053, organisations should have systematic and planned approach to the management of records. As a result the Trust has developed a Records Management Strategy to ensure that from the moment records are created they are properly controlled, readily accessible and available for use until they are eventually archived or otherwise disposed of.

3.7 DH Confidentiality Code of Practice

The NHS Confidentiality Code of Practice is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their health records. It replaces previous guidance. HSG(96) 18/LASSL (96(5 - The Protection and Use of Patient Information, and is a key component of emerging information governance arrangements for the NHS.

3.8 Information Quality Assurance

Information Quality Assurance facilitates a programme of improvement in data quality to ensure that information is fit for purpose. The process reviews the data management processes that are in place to support the collection of patient based data and reviews the outputs from various key systems to measure the accuracy, completeness and validity of that data. For further information please refer to the Data Quality Policy.

3.9 BS10008:2008

BS10008 is the British Standard for evidential weight and legal admissibility of electronic information. The standard sets out requirements for the management of electronic information management systems and the electronic transfer of information between computers. It is anticipated that by conforming to the requirements set out in the standard that the evidential weight of electronic information managed by the Trust will be maximised ensuring its trustworthiness and reliability.

The Trust is currently striving to ensure that all operations undertaken within the new Scanning Bureau (which has been established to support Electronic Medical Records) and their supporting processes and procedures are compliant with BS10008. An application has been submitted for external accreditation by the British Standards Institution and once achieved consideration will be given to extending the scope of compliance across the Trust.

4. RISK MANAGEMENT

4.1 Audit

The Information Governance Group will be responsible for leading on the implementation of Information Governance related Policies and Procedures to ensure that clear formal guidelines have been provided to staff on all aspects of Information Governance. Appendix C shows the Information Governance Policy Framework currently in place. Policies will include mechanisms for monitoring compliance with the policy standards.

4.2 Risks, Incidents and Security breaches

It is the responsibility of departmental managers to ensure that all staff members whether substantive, temporary or voluntary, working within their areas, are fully aware of the

Information Governance Policy and the Information Security Policy and the consequences if security is breached.

It is the responsibility of every staff members to report all actual or suspected security breaches, including near miss incidents that may have placed availability, confidentiality or integrity of information at risk.

Reporting of incidents in this way does not replace the right of staff who may have genuine concerns from pursuing the matter via the Whistle Blowing Policy.

It is imperative that all matters relating to patients, staff, or the financial contractual position of the Trust, remain strictly confidential. Under no circumstances is such information to be divulged or passed to any unauthorised person(s), either intentionally or by failure to comply with the Information Governance Policy.

Failure to observe these rules may be regarded by the Trust as gross misconduct under the 'Policy and Procedure on Conduct and Capability in Employment' and staff should be aware that civil action or criminal proceedings may be instigated as a consequence of damage caused to an individual or organisation.

4.3 Reporting of Serious Incidents relating to Information Security

The reporting of Serious Incidents (SIs) relating to breaches of confidentiality involving personal identifiable data and data losses should be reported in accordance with Basildon and Thurrock University Hospitals NHS Foundation Trust Procedure for Managing Serious Incidents.

5. INFORMATION FOR PATIENTS AND THE GENERAL PUBLIC

5.1 Personal Information

It is a requirement under the Data Protection Act 1998 that all data subjects, which includes both patients and staff are informed

- Of the personal information collected about them
- How the information will be processed
- For what purposes this information will be used

Under the Act processing includes obtaining, storing, recording, altering, retrieving and destroying information. All departments must ensure they have provisions in place for informing patients of how their information will be used. For example attached to registration forms, or on posters or leaflets, available on the Trust Website and displayed as Fair Processing Notices around the Trust.

5.2 Corporate Information

Freedom of Information legislation gives the right of access to all types of information held by the NHS and its partners. It gives the public the right to be told whether the information exists and the right to receive the information

The underlying principle is that all information held by a public authority should be freely available except for a small number of tightly defined exempt items such as personal information, which is governed by the Data Protection Act. It seeks to balance three rights:

- The right to information

- The right to confidentiality
- The right to effective public administration

Under the requirements of the Act the Trust has developed a publication scheme to inform the public of key corporate information held by the Trust.

6. INFORMATION FOR STAFF

The Trust relies on its staff to ensure safe and effective care is given to patients. The Trust is committed to Information Governance and will ensure that security obligations are communicated to all members of staff. It is the responsibility of all staff to maintain Information Governance and ensure that no breaches of Information Governance arise from their actions.

6.1 Personal Information

Staff, like any other individuals, are entitled to know about the personal information held about them. See 5.1

6.2 Confidentiality

Prior to taking up post staff will have been given a 'Confidentiality Form' (Appendix D). Individuals must take responsibility for reading this information and ensuring that they sign the form and return it to the Personnel Department. Job descriptions should also define security roles and the responsibilities of all staff as detailed in this policy. Staff must have a clear understanding of their role and responsibilities in respect of the Information Governance Policy from the outset.
All access to computer systems is conditional upon new members of staff signing a declaration that they are aware of the Information Governance Policy and understand that compliance is a condition of employment

6.3 Staff Training

Departmental managers must ensure that new staff attend Induction Training and understand their responsibilities under Information Governance. All staff must complete the Connecting for Health Information Governance Online Training Tool or equivalent using the Trust NLMS/MOODLE system. This training must be completed on an annual basis. Failure to properly inform an employee of their responsibilities could leave the Trust in a vulnerable position.

6.4 Policies and Procedures

All staff must be made aware of the content and location of relevant policies including the Information security policy and must be allowed time to consider them

6.5 Support Service

There are key members of staff who are available to offer support to staff on all issues in relation to Information Governance. Staff should be made aware that support is available and encouraged to contact the relevant person if they have any concerns regarding Information Governance issues. A list of useful contact number is provided in Appendix B.

7. CONSULTATION, APROVAL AND RATIFICATION

This procedure has been approved by the Information Governance Group

8. DISSEMINATION AND IMPLEMENTATION

All staff will be affected by the implementation of this procedure. Implementation will be co-ordinated by the Information Governance Manager.

9. REVIEW AND REVISION ARRANGEMENTS INCLUDING VERSION CONTROL

This procedure will be reviewed three yearly (or sooner if new legislation, codes of practice or national standards are to be introduced). The version of the document will be changed in line with the Trust's Controlled Document Policy/Procedure.

10. DOCUMENT CONTROL INCLUDING ARCHIVING ARRANGEMENTS

Once this procedure is superseded a copy will be retained in the Trusts Document Management System archives for a minimum of 10 years in line with the recommendations contained within “Records Management: NHS Code of Practice” (2006).

Appendix A

Relevant Legislation, NHS Guidance and Trust Policies

Legislation

- The Data Protection Act 1998
- Computer Misuse Act 1990
- Access to Health Records Act 1990
- Access to Medical Reports Act 1988.
- The Human Rights Act 1998
- The Freedom of Information Act 2000
- Health Act 1999
- Health and Safety at Work Act 1974
- Health & Social Care Act 2001
- Mental Capacity Act 2005
- Crime and Disorder Act 1998
- Public Records Act 1958/1967
- Children Act 2004
- Electronic Communications Act 2000
- Copyright, design and patents Act 1998
- Regulation of Investigatory Powers Act 2000

For more information on the above and other Legislation see www.legislation.hmso.gov.uk

NHS Guidance

- Introduction to the Data Protection in the NHS (IMG E5127)
- Confidentiality: NHS Code of Practice Nov 2003
- Access to health records under Data Protection Act 1998 version 2
- Information for Health: An information strategy for the modern NHS 1998–2005
- DH Records Management Code of Practice
- Section 60 Health & Social Care Act 2001
- The Caldicott Committee Report
- Caldicott Guardians HSC 1999/012
- Information Security Management - BS7799
- BS7799 – A code of practice for Information Security
- NHSnet: Equipment Disposal & Data Destruction
- Department of Health Standards for better Health
- DH Information Security Management Code of Practice April 2007

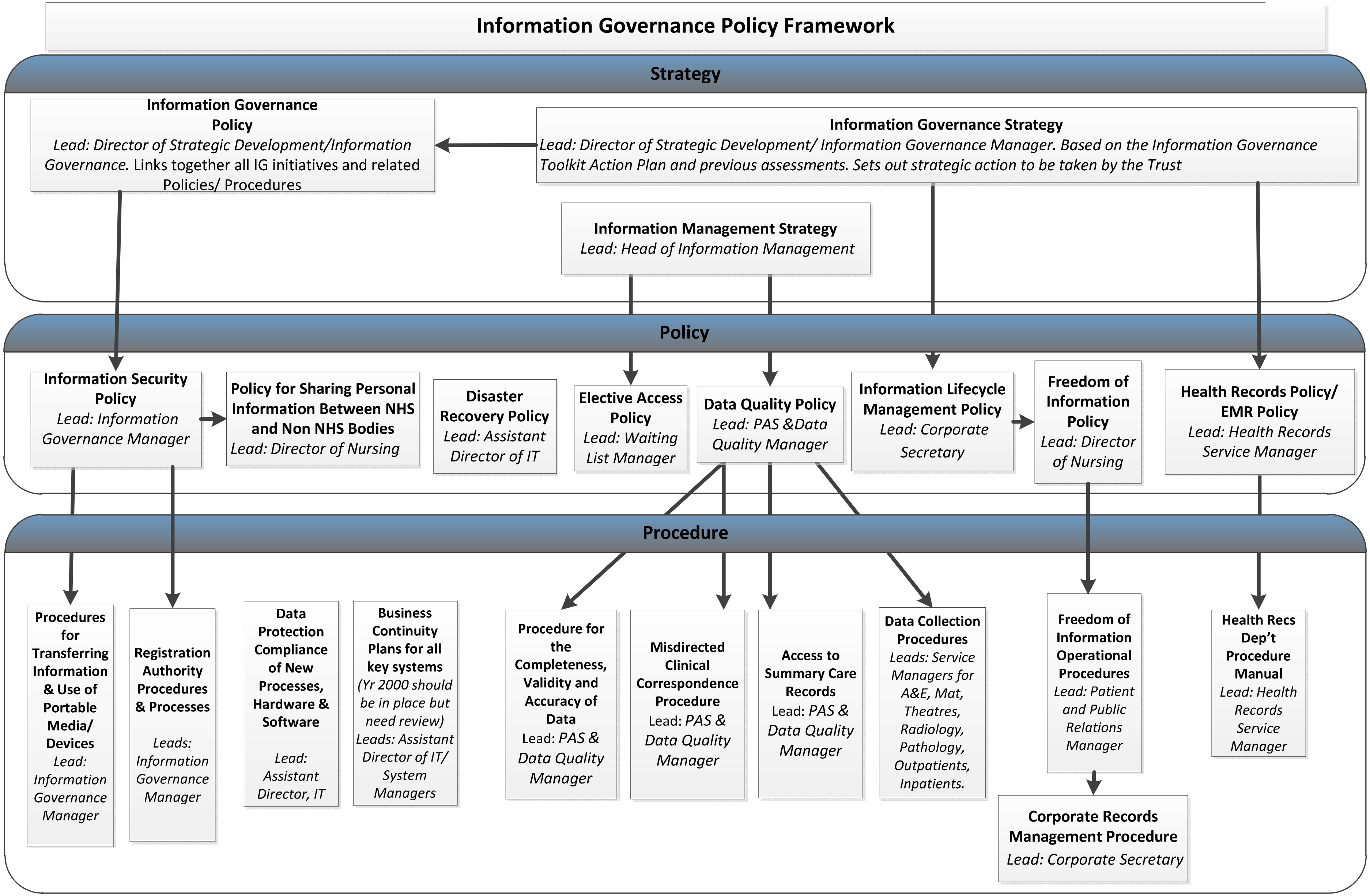
For more information on NHS Guidance see www.dh.gov.uk/PolicyAndGuidance/

Appendix B

CONTACT NUMBERS

1. Director Of Nursing (Caldicott Guardian)	Ext. 1292
2. Senior Information Risk Owner	Ext 1301
3. Information Governance Manager	Ext. 1957
4. IT Projects Manager	Ext. 8103
5. Corporate Secretary	Ext. 3303
6. Freedom of Information Facilitator	Ext. 3057
7. Health Records Manager	Ext. 5086
8. Assistant Director of IT	Ext. 1919
9. PAS & Data Quality Manager	Ext. 1977

Appendix C



Information Governance Policy Framework

Strategy

Information Governance Policy
Lead: Director of Strategic Development/Information Governance. Links together all IG initiatives and related Policies/ Procedures

Information Governance Strategy
Lead: Director of Strategic Development/ Information Governance Manager. Based on the Information Governance Toolkit Action Plan and previous assessments. Sets out strategic action to be taken by the Trust

Information Management Strategy
Lead: Head of Information Management

Policy

Information Security Policy
Lead: Information Governance Manager

Policy for Sharing Personal Information Between NHS and Non NHS Bodies
Lead: Director of Nursing

Disaster Recovery Policy
Lead: Assistant Director of IT

Elective Access Policy
Lead: Waiting List Manager

Data Quality Policy
Lead: PAS &Data Quality Manager

Information Lifecycle Management Policy
Lead: Corporate Secretary

Freedom of Information Policy
Lead: Director of Nursing

Health Records Policy/ EMR Policy
Lead: Health Records Service Manager

Procedure

Procedures for Transferring Information & Use of Portable Media/ Devices
Lead: Information Governance Manager

Registration Authority Procedures & Processes
Leads: Information Governance Manager

Data Protection Compliance of New Processes, Hardware & Software
Lead: Assistant Director, IT

Business Continuity Plans for all key systems
(Yr 2000 should be in place but need review)
Leads: Assistant Director of IT/ System Managers

Procedure for the Completeness, Validity and Accuracy of Data
Lead: *PAS & Data Quality Manager*

Misdirected Clinical Correspondence Procedure
Lead: *PAS & Data Quality Manager*

Access to Summary Care Records
Lead: *PAS & Data Quality Manager*

Data Collection Procedures
Leads: Service Managers for A&E, Mat, Theatres, Radiology, Pathology, Outpatients, Inpatients.

Freedom of Information Operational Procedures
Lead: Patient and Public Relations Manager

Corporate Records Management Procedure
Lead: Corporate Secretary

Health Recs Dep't Procedure Manual
Lead: Health Records Service Manager

Appendix D

CONFIDENTIALITY CODE OF CONDUCT FOR STAFF

This following confidentiality Code of Conduct applies to all staff working for the Trust and will include bank, voluntary, locum, agency, student placements and temporary staff. It is important that the following information is read and understood prior to signing a contract of employment with the Trust.

PURPOSE OF THE CODE

All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities and where applicable their own professional code/s of conducts, but also a requirement of the Data Protection Act 1998, the Department of Health Confidentiality Code of Practice issued in November 2003, and the NHS Care Records Guarantee.

- The Trust is committed to the delivery of a first class confidential service. This means ensuring that all information is processed fairly, lawfully and as transparently as possible so that patients, staff and the public:

- Understand the reasons for processing information
- Give their consent for the disclosure and use of their personal information
- Gain trust in the way the Trust handles information
- Understand their rights to access information held about them

In the course of your duties you may have access to confidential information about patients, staff or Trust business in general. Under no circumstances must personal information about patients be divulged to anyone other than authorised persons, e.g. nursing or other health professional staff, who are concerned directly with the care, diagnosis/or treatment of the patient.

Similarly, information of a personal or confidential nature concerning individual staff members must not be divulged to anyone unless there is a genuine justified purpose to access this information as part of their job role, and where necessary appropriate authority has been given to release the information.

Failure to observe these rules will be regarded by the Trust as gross misconduct and could result in serious disciplinary action being taken against you, including dismissal.

SIGNATURE OF AGREEMENT

I agree to observe the strictest confidence with regard to any information, which relates to the Trust business, patients or staff that I have access to, or accidentally gain knowledge of, in the course of my duties.

I agree that I will not use any information for any purpose that is outside the responsibilities of my work.

I agree not to access any records containing personal information unless I have a legitimate need to do so.

I understand that a breach of these rules could lead to serious disciplinary action, up to and including dismissal, being taken against me.

I acknowledge receipt of the guidance notes on confidentiality, printed on the reverse of this code, and I agree to adhere to the Trust Information Security Policy at all times during the course of my work.

Signed ………………………………………………. Date……………………………………...

Print Name ……………………………………………….. Job Title……………………………………

KEY POINTS ON CONFIDENTIALITY

- Detailed below are some important key points on confidentiality. Further information is provided in the Trust Information Security Policy. It is your responsibility to ensure that you read, understand and adhere to this policy at all times. Training in the application of this policy in your own area of work is available. If you need further advice on any issues relating to Information Security and Confidentiality or would like to book training you should speak to your line manager or telephone the Information Governance Manager on ext. 1957.

WHAT IS CONFIDENTIAL INFORMATION?

- Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored.

- For example, information may be held on paper, floppy disc, CD, computer file or printout, video, photograph or even heard by word of mouth.

- It includes information stored on portable devices such as laptops, palmtops, mobile phones and digital cameras.

- It can take many forms including medical notes, audits, employee records, occupational health records etc. It also includes any corporate information, such as Trust confidential information.

- Person-identifiable information is anything that contains the means to identify a person, such as name, address, postcode, date of birth, NHS number or National Insurance number. Even a visual image (e.g. photograph) is sufficient to identify an individual.

- Certain categories of information are legally defined as particularly sensitive and should be carefully protected by additional requirements stated in legislation such as information relating to fertilisation, sexually transmitted diseases, HIV or termination of pregnancy.

- During your duty of work you should consider all information to be sensitive, even a patients name and address. The same standards should be applied to all information you come into contact with.

WHAT MUST BE DONE TO MAINTAIN CONFIDENTIALITY?

- Comply with relevant Trust Policies such as the Trust Information Security Policy.
- To undertake the mandatory training module(s) on the Connecting for Health Information Governance Online Training Tool (http://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm) on an annual basis.
- Keep all work areas secure.
- Confidential information must not be left lying around on desks, photocopiers or printers.
- Staff must wear their photo ID at all times whilst on duty.
- Equipment data or software must not be removed from site without relevant permissions.
- PCs must be logged off when not in use.
- Passwords must not be shared.
- Confidential information must be disposed of securely.
- When it is necessary to verbally pass on or check confidential information, care should be taken that it is not disclosed to unauthorised third parties. Do not give out any information to the police or media without seeking advice from a senior member of staff.
- Fax, e-mail must only be used to transfer confidential information within prescribed guidelines.
- Information Security Incidents and Breaches mush be reported to your line manager and by completion of the Trusts Incident Reporting Form.
- Take individual responsibility for your actions and understand and comply with the Law.
- Information Security Risks must be reported to your line manager and Directorate Information Security Lead.
- The signing of these documents does not exclude staff who have genuine concerns pursuing the matter via the Trusts ‘Whistle Blowing Policy’