Information Governance Policy

Department / Service:	Information
Originator:	Information Governance Manager
Accountable Director:	Chief Finance Officer
Approved by:	Information Governance Steering Group
Date of Approval:	19th December 2018
Review Date: **This is the most current document and should be used until a revised version is in place**	19th December 2020
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	All
Target staff categories	All

Policy Overview:
This policy provides the Information Governance Framework required for compliance with relevant legislation, and for effective management and protection of organisational and personal information.

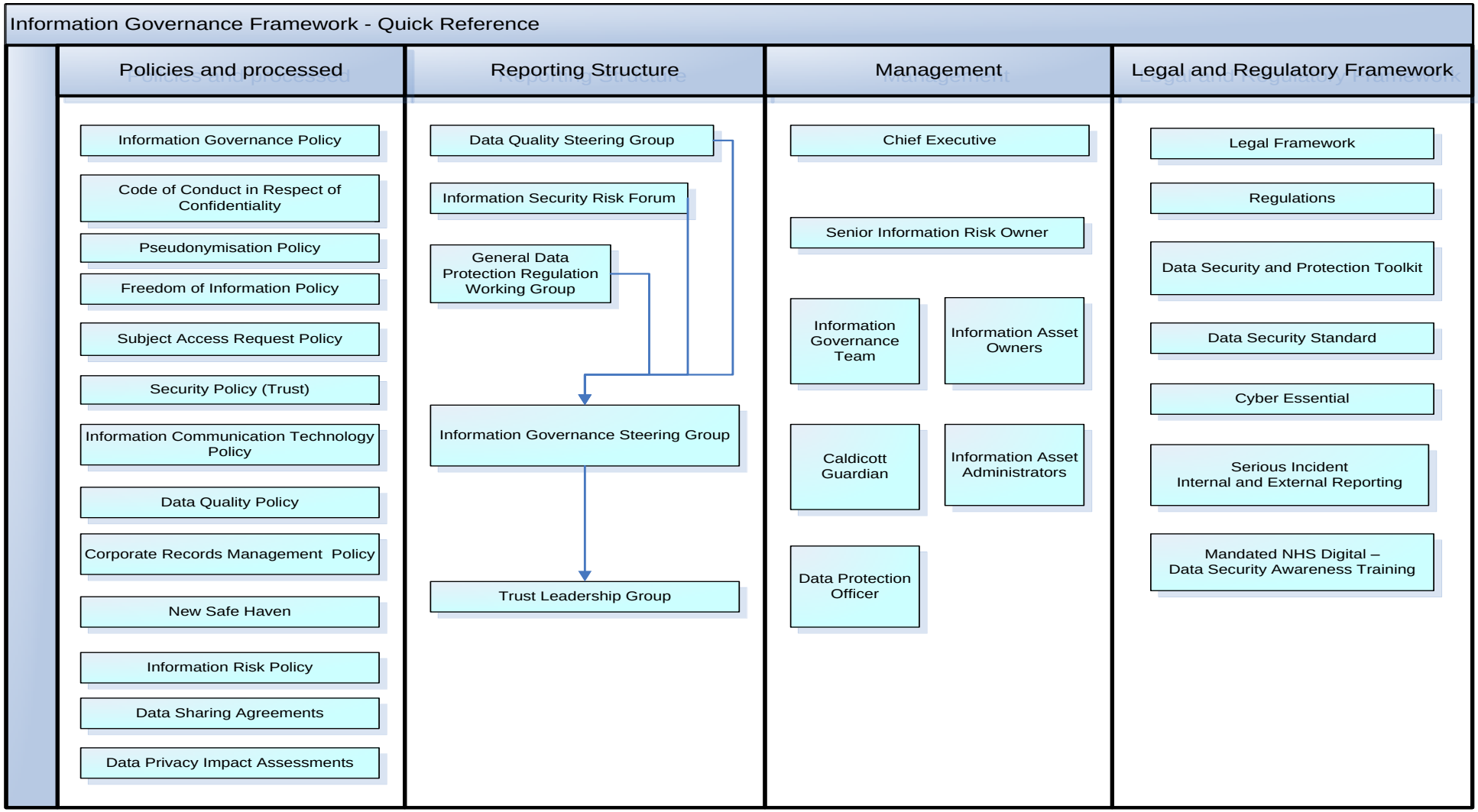
Latest Amendments to this policy:
This policy has been rewritten to reflect the latest legislation and national requirements and is a combination of an Information Governance Policy and Strategy

Contents page:

Appendices

Supporting Documents

Supporting Document 1	Equality Impact Assessment
Supporting Document 2	Financial Risk Assessment


Information Governance Framework - Quick Reference
Policies and processed
Information Governance Policy
Code of Conduct in Respect of Confidentiality
Pseudonymisation Policy
Freedom of Information Policy
Subject Access Request Policy
Security Policy (Trust)
Information Communication Technology Policy
Data Quality Policy
Corporate Records Management Policy
New Safe Haven
Information Risk Policy
Data Sharing Agreements
Data Privacy Impact Assessments
Reporting Structure
Data Quality Steering Group
Information Security Risk Forum
General Data Protection Regulation Working Group
Information Governance Steering Group
Trust Leadership Group
Management
Chief Executive
Senior Information Risk Owner
Information Governance Team
Information Asset Owners
Caldicott Guardian
Information Asset Administrators
Data Protection Officer
Legal and Regulatory Framework
Legal Framework
Regulations
Data Security and Protection Toolkit
Data Security Standard
Cyber Essential
Serious Incident Internal and External Reporting
Mandated NHS Digital – Data Security Awareness Training

INFORMATION GOVERNANCE STRATEGY

Strategy statement:
This strategy sets out the approach taken within Worcestershire Acute Hospitals NHS Trust (the Trust) to provide a robust Information Governance (IG) Management Framework, for the current and future management of information, and compliance with required legislation.

This strategy sets out to further develop and implement a change in culture towards IG by all staff. IG is a key component of performance management, i.e. it is central to the working practices of all staff, of all grades and roles, permanent or temporary, working within the Trust.

Through the implementation of the IG Policy, the Trust will:

1. Establish robust information governance processes conforming to the law, NHS and Department of Health standards
2. Ensure that all policies and procedures relating to the processing of personal information, including handling and holding personal and Trust corporate information are legal and conform to best and/or recommended practice. This includes completing a Privacy Impact Assessment for the implementation of any new systems or change of process
3. Complete and maintain a record of all data flow's containing personal information and ensure Data Sharing Agreements are in place and signed off where required.
4. Ensure that clear information is given to patients, families and carers, and staff about how their personal information is recorded, handled, stored and (if required) shared by the Trust. The public will be provided with guidance, available in various formats, to explain their rights, how their information is handled, how they can obtain further information and how they can raise concerns. This is published in the Privacy Notice that is included on the Trust website
5. Provide clear advice and guidance to staff and ensure that they understand and apply the principles of Information Governance to their working practices in relation to protecting the confidentiality and security of both personal and business information. To ensure the safekeeping and secure handling of information, and compliance with appropriate legislation, Information Governance and Data Security Essentials have been provided and must be followed.
6. Ensure that procedures are reviewed on a regular basis to monitor their effectiveness in order that improvements or deficiencies in information handling standards can be recognised and addressed
7. Work to embed an Information Governance culture in the Trust through increasing awareness and providing training on the key issues
8. Maintain a clear reporting structure and ensure that through management action and training all staff understand the IG requirements
9. Undertake regular reviews and audits of how information is recorded, held and used. Audits will be used to identify good practice
10. Ensure that there are robust procedures for notifying and learning from IG breaches and incidents in line with the Incident Reporting Policy
11. Ensure an action plan is developed and agreed in response to the Data Security and Protection Toolkit, developing and taking forward improvement plans pertaining to the current toolkit, and reporting progress to the Information Governance Steering Group on a regular basis.
12. Ensure that the National Data Security Standards are embedded in the IG culture, including continuing to highlight and manage/mitigate risks to cyber security.

Implementation of these strategic aims and objectives are included in the policy and in associated documents (guidance, standards and procedures), and by the annual submission of the Data

Security and Protection Toolkit. This work is monitored, reviewed and signed off by the Information Governance Steering Group

The Trust needs to ensure it is taking into account the changes taking place in IG both across the local landscape and nationally that will impact on IG in the next 1 to 3 years. These will include;

What do WAHNT need to be ready to support in the long term (2021-2023)

- Data Sharing across NHS and public sector boundaries
- Integrated Health Record
- Data Sharing Agreements with partner organisations (including non-NHS)
- Technical infrastructure across the health economy
- Increased cyber security risk

Considerations and dependencies

- Integration with ICT Strategy
- Data security agenda
- Resource
- Dealing with organisational sensitive data as well as PII

Year 1 focus (2018/19)

Organisational Ownership and knowledge

- Divisional triumvirate ownership

(DMDs – Caldicott, DOps – IAO training)

- Embed IAO / IAA structure
- Accredited training for different levels of the organisation

GDPR Compliance

- Data mapping (identification of PII)
- Data Sharing Agreements
- Privacy by Design
- Cyber security compliance
- Learning from data breaches

Data Integrity

- FOMI assurance
- Data quality flagging
- Information Management Policy

Year 2 and 3 focus (2019/21)

Paper light agenda

- Infrastructure support and guidance
- Integration with WAHNT ICT Strategy
- National paperless 2021

Records retention management

- Continued GDPR compliance
- Health, corporate and HR records retention

1. Introduction

This policy provides the Information Governance Framework required ensuring compliance with relevant legislation, and for effective management and protection of organisational and personal information.

Information is the most important asset available to an organisation and therefore all organisations must have robust arrangements for Information Governance (IG) which are reviewed annually and described in the Data Security and Protection Toolkit (DS&PT).

Information Governance is owned by the Trusts most senior management and this is demonstrated by signing annually a Statement of Compliance via the DS&PT in respect to the Trust and any contracted services.

The DS&PT is based upon the 10 Data security standards detailed in section 5 of this policy.

IG Compliance is supported by the key roles of Caldicott Guardian, Senior Information Risk Owner (SIRO), Data Protection Officer (DPO) and Information Governance Manager (IGM) who is supported by the Information Governance Officer. However, all staff has a duty of confidentiality, and an important role to play in ensuring the Trust achieves its strategic objectives.

IG Compliance is also supported by the identification of Information Asset Owners, Administrators, Information Mapping and Information Asset Registers through a process of risk management.

2. Scope of this document

All staff within the trust, both permanent and temporary, who either use information “owned” by the Trust, or requiring access to information “owned” by the Trust.

3. Definitions

IG	The term **Information Governance** describes the structures, policies and practices used to ensure the confidentiality and security of patients/service users; employment records relating to staff and Trust corporate business.
Information	“**Information**” includes information in any media - including paper records and electronic data: clinical records, letters, emails, CDs, DVDs, x-rays, patient administration systems; corporate information including staff records; financial records and estates and facilities records. This includes the equipment that gathers or stores the above – e.g. computers (networks, desktops), laptops, smart phones, paper records stores.
IGSG	**Information Governance Steering Group** Forum to discuss / agree all information Governance issues and policies.
PCD	**Person Confidential Data** This is a term used in healthcare regarding information/data about a person which a person would expect to be held in confidence and would enable that person’s identity to be established by one means or another. Name and address are very strong identifiers, particularly when available together and medical data would be an example of confidential information.
PII	**Personally Identifiable Information**

	A term used in data protection to describe information which identifies an individual.
SIRO	**Senior Information Risk Owner** Named director who has overall responsibility for information risks within the Trust
IAO	**Information Asset Owner** Executives for each directorate / area responsible for identifying and reporting information assets/risks
IAA	**Information Assess Administrator** Operational manager for information systems, reporting to the IAO
Caldicott Principles	A set of principles that apply to all confidential information (resulting from Caldicott Reviews)
GDPR	General Data Protection Regulation
DPO	Data Protection Officer
DS&PT	Data Security and Protection Toolkit

4. Responsibility and Duties

Board Responsibility
The Chief Executive as Accountable Officer has overall accountability and responsibility for information governance 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 governance, are effectively managed and mitigated.

Senior Information Risk Officer (SIRO)
The SIRO will provide an essential role in ensuring that identified information threats are followed up and incidents managed. They will also ensure that the Board and the Accountable Officer are kept up to date on all information risk issues. The role will be supported primarily by the Information Asset Owners, who will report any risks directly to the SIRO. Further support will be provided by the Caldicott Guardian, ICT Service Delivery Manager, Information Governance Manager and Officer.

Caldicott Guardian
The Caldicott Guardian is responsible for ensuring that the Caldicott Principles are followed – refer to the Code of Conduct in Respect of Confidentiality.

Data Protection Officer
The Data Protection Officer provides the organisation independent risk-based advice to support its decision-making in the appropriateness of processing Personal and Special Categories of Data within the Principles and Data Subject Rights laid down in the General Data Protection Regulation (GDPR).

The Assistant Director of Information and Performance is responsible for identifying any resources required for year on year improvements identified in the DS&PT.

The Information Governance Manager is responsible for overseeing day to day information governance issues; developing and maintaining policies, standards, procedures and guidance

Information Asset Owners/Administrators are responsible for identifying and reporting information assets/risks

All Managers within the Trust are responsible for ensuring that the policy and supporting standards and guidelines are built into local processes to ensure on-going compliance.

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

5. Policy Detail

Legal and Regulatory Framework
There are a number of legal obligations placed upon the Trust for the use and security of personal and confidential information. The EU General Data Protection Regulations (GDPR) came into force in May 2018. Additionally, the Data Protection Act 1998 has been replaced by a new UK Data Protection Act is due for implementation.

The Trust is registered with the Information Commissioners Office as a Data Controller and processor of information, and must comply with its duties as defined by this registration.

Legal and Regulatory Framework:
The Trust is bound by the provisions of a number of laws and regulations. The list below is not exhaustive, and other legislation and regulations may also apply.
Laws:

- UK Data Protection Act 2018
- General Data Protection Regulations
- Health & Social Care (Quality & Safety) Act 2015
- Common Law Duty of Confidentiality
- Health & Social Care Act 2012
- National health Service Act 1977 / 2006
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Crime and Disorder Act 1998
- Road Traffic Act 1988
- Electronic Communications Act 2000
- Public Interest Disclosure Act 1998
- Public Records Act 1958, 1967 and 2005

Regulations:

- Caldicott Committee Report 2013
- NHS Confidentiality Code of Practice 2003
- DoH Records Management: Code of Practice 2016
- NHS Digital – Data Security & Protection Toolkit – National Data Security Standards
- Care Quality Commission Standards

The aim of the policy and management framework is to ensure compliance with the strategic objectives and legal obligations above and DS&PT requirements. A schedule of DS&PT compliance is an integral part of the action plan which is regularly reviewed and updated at the Information Governance Steering Group (IGSG).

National Data Security Standards

The agenda of the IGSG is structured around the National Data Guardian's 10 Data Security Standards:

Leadership Obligation 1	
People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles	
Data Security Standard 1	All staff ensures that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes
Data Security Standard 2	All staff understands their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
Data Security Standard 3	All staff complete appropriate annual data security training and pass a mandatory test, provided through the redesigned Data Security and Protection Toolkit (or provide similar via in-house training programmes)
Leadership Obligation 2	
Process: Ensure the organisation proactively prevents data security breaches	
Data Security Standard 4	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
Data Security Standard 5	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
Data Security Standard 6	Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
Data Security Standard 7	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
Leadership Obligation 3	
Technology: Ensure technology is secure and up-to-date.	
Data Security Standard 8	No unsupported operating systems, software or internet browsers are used within the IT estate.
Data Security Standard 9	A strategy is in place for protecting IT systems from cyber threats which are based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
Data Security Standard 10	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Information Governance Steering Group
The Information Governance Group (IGSG) is accountable to the Trust Leadership Group (TLG), and has responsibility to ensure the Trust adheres to the Information Governance Policy. There are three subgroups which report into IGSG; Data Quality Steering Group; Information Security Risk Forum and the General Data Protection Regulation Working Group.

The IGSG agenda is structure to monitor compliance with the National Data Security Standards (above) and sign off completion of the NHS Digital Data Security & Protection Toolkit.

The purpose and functions of the IGSG are set out in the IGSG Terms of Reference. The terms of reference are updated annually. For further information contact the Information Governance team.

Incident reporting:
Failure to comply with this policy may result in breaching the GDPR/Data Protection Act (and other legal and regulatory) requirements, resulting in a fine from the Information Commissioner. Where there is a breach of confidentiality or loss of data or information asset, this must be reported and managed via the incident reporting process (via the incident reporting system Datix).

All serious incidents, known as IG SIs, that are rated as Level 2 or above, must be recorded and reported via the NHS Digital Incident Reporting Tool on the NHS Digital DS&PT. This will automatically result in a referral to the Information Commissioner's Office. Any potential Level 2 incident will be assessed using the Trusts serious incident reporting process managed by the Information Governance (IG) team. Once this is completed, and the severity rating of Level 2 is confirmed, the IG Team will then inform the Head of Information and performance, SIRO, Data Protection Officer and Caldicott Guardian before reporting the incident externally.

The IG Team will update the NHS Digital DS&PT reporting tool on a regular basis with regard to the management of the incident, and any response received from the Information Commissioners Office regarding the outcome. Once all actions have been taken to manage the incident, mitigate any risks, and implement the agreed action plan, the incident will be closed.

The Information Governance Steering Group will receive regular reports of incidents; analysis of trends and review copies of Incident Management Reports to ensure the mitigation of the risk, and share learning across the Trust.

Training Requirements

All new staff will attend an information governance awareness session as part of their Induction. During the session staff will be informed that Data Security training is mandatory and must be completed using the on line Data Security Awareness training accessed in ESR. Ancillary staff will complete the same training using a paper version which is sent to the Information Governance team to be inputted manually into ESR.

Annual mandatory on-line Data Security Awareness training is mandatory for all employed staff (both permanent and temporary).

In addition some roles are required to complete additional annual training, (e.g. the Data Protection Officer; SIRO, Caldicott Guardian, IT Security Specialist) as detailed in the Training Needs Analysis

The Board are required to receive risk management training.

Compliance with the mandatory annual training is monitored by the Data Quality team and staff receives email reminders if they have completed their training via ESR.

Data Privacy Impact Assessments (DPIA)

A number of processes and procedures apply to Information Governance and all staff should be aware of the procedures applicable when implementing any change to the way the Trust collates, processes or shares information. Staff should be aware that there can be no change to service delivery without appropriate Information Governance sign off.

A Data Privacy Impact Assessment is required when a proposed change to service delivery involves the way the Trust collates, processes or shares information.

The General Data Protection Regulation (GDPR), which came into force on the 25th of May 2018, makes PIAs or data protection impact assessments (DPIA) mandatory for organisations whose practices and technology create a high level of risk to the privacy rights of its data subjects. Organisations must be able to demonstrate that a PIA has been carried out, or penalties can be enforced against the organisation.

General guidance is available about the completion of a DPIA on the IG webpage and further advice and guidance may be obtained from the Information Governance Team

Data Processing Agreement (DPA)

If a DPIA shows that data needs to be shared and this may have an impact on the privacy of individuals, it will be necessary for an ISA or DPA to be put in place. The ISA or DPA will need to be approved by the Caldicott Guardian and Senior Information Risk Owner (SIRO) and signed by the SIRO or Deputy SIRO.

6. Implementation

6.1 Plan for implementation

The Trust will ensure the policy is implemented via the Data Security and Protection Toolkit action plan. The policy will be supported by Information Governance training, awareness and suite of policies. The Information Governance policies will be approved and monitored by the Information Governance Steering Group.

6.2 Dissemination

This policy will be published on the Trust's Intranet. It is the responsibility of line managers to ensure that members of staff are made aware of this policy. New members of staff are advised during their induction process to look at the Trusts Intranet to ensure that they read and have a good working knowledge of all relevant policies, strategies, procedures and guidelines. The Information Governance Manager will ensure that the policy is publicised via an article on the Trusts Weekly Brief

6.3 Training and awareness

Annual Data Security Awareness Training is mandatory and covers all areas of this policy

6.4 Monitoring and compliance

See table below

Page/ Section of Key Document	Key control:	Checks to be carried out to confirm compliance with the Policy:	How often the check will be carried out:	Responsible for carrying out the check:	Results of check reported to: *(Responsible for also ensuring actions are developed to address any areas of non-compliance)*	Frequency of reporting:
	WHAT?	**HOW?**	**WHEN?**	**WHO?**	**WHERE?**	**WHEN?**
	Completion of the Data Security and Protection Toolkit	Submission • Baseline – 31st July • Performance Review – 31st October • Submission of self-assessment for the year – 31st March	See 'How' Box	Information Governance Manager	• Information Governance Steering Group • Trust Leadership Group	See 'How' box
	External Audit of the DS&PT	Agreed IG days in the Trust audit plan annually	Agreed in advance	Information Governance Manager	• Information Governance Steering Group • Trust Leadership Group • Audit Committee	Annually
	Statement of Internal Control					
	Reviewing all IG Incidents	Assessed on DATIX incident reporting process	As they occur	Information Governance Manager	Managing all incidents and assessing for potential IG SI's	As they occur
	Escalating all IG SI's	Assessed via the IG reporting process and reported on the DS&PT (including reported in the ICO)	As they occur – strict reporting time scales are set via ICO	Information Governance Manager	Reported to CG/DPO/IGSG/SIRO and included in the TLG reports	As they occur

	General compliance to IG Standards	DS&PT Action Plan	Every IGSG	Information Governance Manager	• Information Governance Steering Group • Trust Leadership Group	Every IGSG

7. Policy Review

This policy will be reviewed biannually by the Information Governance Manager and relevant key staff

8. References [You should include external source documents and other Trust documents that are related to this Policy]

References:	Code:
Code of Conduct for Employees in Respect of Confidentiality	
Incident Reporting Policy	
Complaints and PALS Policy and Procedure	
Freedom of Information Policy	
IG related polices and guidance	
Caldicott Review/Principles	
Data Security and Protection Toolkit	

9. Background

9.1 Equality requirements

The assessment conducted for this policy reveals no equality issues. See supporting document 1

9.2 Financial risk assessment

A financial risk assessment has been performed and reveals there are no financial implications to this policy. See supporting document 2

9.3 Consultation

The policy has been updating by the Information Governance Manager with input from the Information Governance Steering Group members.

Contribution List

This key document has been circulated to the following individuals for consultation;

Designation
Chief Finance Officer (SIRO)
Caldicott Guardian
Assistant Director of Information and Performance
Company Secretary and Data Protection Officer
Head of Operational IT
Information Governance Officer
Head of Human Resource's - Workforce
Head of Legal Services

This key document has been circulated to the chair(s) of the following committee's / groups for comments;

Committee
Information Governance Steering Group

Key Documents Approval Group

9.4 Approval Process

This policy is agreed by the Information Governance Steering Group and then finally approved at Key Documents Approval Group (KDAG). Minor changes can be approved by the SIRO via the IGSG prior to the 2 year review.

9.5 Version Control

This section should contain a list of key amendments made to this document each time it is reviewed.

Date	Amendment	By:
Sept 2010	Document created	Information Governance Manager
Nov 2012	General update into latest policy template and minor amendments to content (Version 2)	Information Governance Manager
July 2014	General update into latest policy template and minor amendments to content (Version 3)	Information Governance Manager
Sept 2016	Updated specified years (2014/2016) to cover current policy approval Updated reporting structure and approval process Updated Caldicott Function appendix Updated reference section with updated trust policies Updated PCD appendix and reference to PID throughout policy	Information Governance Manager
Dec 2018	This policy has been rewritten to reflect the latest legislation and national requirements and is a combination of the Information Governance Policy and Strategy	Information Governance Manager

Supporting Document 1 - Equality Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the Policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4.	**Is the impact of the Policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	N/A	
6.	**What alternatives are there to achieving the Policy/guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	

If you have identified a potential discriminatory impact of this key document, please refer it to Assistant Manager of Human Resources, together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact Assistant Manager of Human Resources.

Supporting Document 2 – Financial Impact Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	Yes/No
1.	Does the implementation of this document require any additional Capital resources	No
2.	Does the implementation of this document require additional revenue	No
3.	Does the implementation of this document require additional manpower	No
4.	Does the implementation of this document release any manpower costs through a change in practice	No
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No
	Other comments:	

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval