Trust Policy	NHS Worcestershire Acute Hospitals NHS Trust

Corporate Records Management Policy and Procedure

Department / Service:	Corporate
Originator:	Information Governance Manager
Accountable Director:	Chief Finance Officer
Approved by:	Information Governance Steering Group (IGSG) Trust Management Executive
Date of approval:	10th June 2019
First Revision Due:	10th December 2020
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	All
Target staff categories	All

Policy Overview:

This policy defines a structure for Worcestershire acute services to ensure records are maintained, managed and controlled effectively and at best value, commensurate with legal, operational and information needs. This policy is designed to provide all professionals working within Worcestershire Acute Trust with information on the principles of good documentation and record keeping within their administrative and clinical practice and ensure consistent standards across professional groups.

Latest Amendments to this policy:

Minor update including, relevant dates and approval
Appendices removed and available on the Information Governance Webpages
12th June 2020 – Document extended for 6 months whilst in order to have the resource to update and consider any local or national changes to be incorporated.

Contents page:

Appendices
None

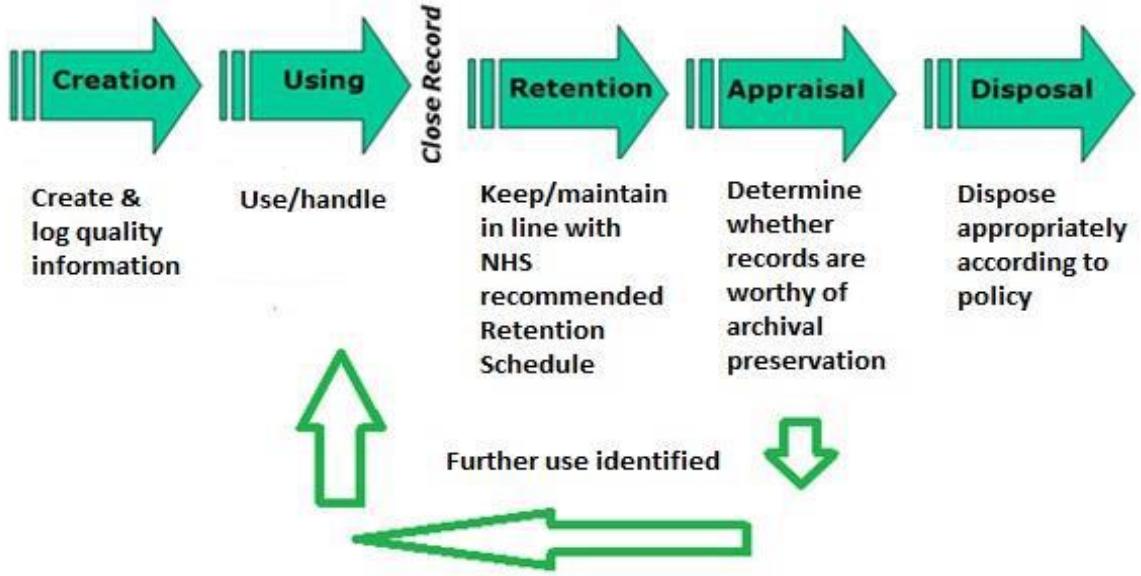
Supporting Documents

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

Quick Reference Guide

This policy sets out the structure for the trusts corporate records

The Records / Information Lifecycle
The records lifecycle, or the information lifecycle, is a term that describes a controlled regime in which information is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest. This can be seen diagrammatically in Figure 1.



Record characteristic	How to evidence
Authentic	• It is what it purports (claims) to be • To have been created or sent by the person purported to have created or sent it and • To have been created or sent at the time purported.
Reliable	• Full and accurate record of the transaction/activity or fact • Created close to the time of transaction/activity • Created by individuals with direct knowledge of the facts or by instruments routinely involved in the transaction /activity.
Integrity	• Complete and unaltered • Protected against unauthorised alteration • Alterations after creation can be identified as can the persons making the changes.
Useable	• Located, retrieved, presented and interpreted • The context can be established through links to other records in the transaction/activity.

1. Introduction

1.1 Worcestershire Acute NHS Trust is dependent on its records to operate efficiently and to account for its actions. This policy defines a structure for Worcestershire acute services to ensure adequate records are maintained, managed and controlled effectively and at best value, commensurate with legal, operational and information needs. This policy is designed to provide all professionals working within Worcestershire Acute Trust with information on the principles of good documentation and record keeping within their administrative and clinical practice and ensure consistent standards across professional groups.

1.2 Our organisation's records are our corporate memory, providing evidence of actions and decisions and representing a vital asset to support our daily functions and operations. They support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public who have dealings with us. They support consistency, continuity and efficiency and productivity and help us deliver our services in consistent and equitable ways.

1.3 The Public Records Act 1958 requires that all public bodies have effective management systems in place to deliver their functions. For health and social care, the primary reason for managing information and records is for the provision of high quality care. The Secretary of State for Health and all NHS organisations have a duty under this Act to make arrangements for the safe keeping and eventual disposal of all types of records. This is carried out under the overall guidance and supervision of the Keeper of Public Records, who is answerable to Parliament.

1.4 An effective corporate records policy ensures that such information is properly managed and available to support:

- Patient care
- The day-to-day business, which underpins care delivery.
- Evidence-based practice/care pathways.
- Management decision-making.
- Legal requirements including Data Protection Act and Freedom of Information Act, Equal Opportunities Act.
- Medical, organisational and miscellaneous audits.
- Improvements in clinical effectiveness through research.
- Single Assessment Process
- Clinical Governance
- Research Governance
- Reduction in aspects of risk
- Equality Legislation

1.5 Records management, through the proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater coordination of information and storage systems.

1.6 All NHS records are Public Records under the Public Records Acts and must be kept in accordance with following statutory and NHS guidelines:

- Public Records Acts 1958 and 1967
- Data Protection Act 1998
- Freedom of Information Act 2000
- NHS Code of Practice on Confidentiality
- Records Management Code of Practice for Health and Social Care 2016
- NHS Resolution (Formerly NHSLA)
- Clinical Negligence Scheme for Trusts (CNST) (relating to maternity)
- Care Quality Commission
- Audit Commission, Setting the Record Straight, 1995
- Information Security Management: NHS Code of Practice
- Standards for the clinical structure and content of patient records
- Independent Inquiry into Child Sexual Abuse (IICSA),

Where records are to be shared with other organisations (e.g. social services) this must be done in accordance with documented and agreed information sharing protocols. In respect of Health and Social Services, Worcestershire has in place information sharing protocols for both Adults and Children and Young people. A copy of these documents can be found on the intranet website.

2. Scope of this document

2.1 This policy relates to all operational records.

The ISO standard, ISO 15489-1:2016 Information and documentation - Records management defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'.

The Data Protection Act 1998 (DPA) S68(2) defines a health record which 'consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual'.

Examples of records that should be managed using the guidelines in this Code are listed below. This list gives examples of functional areas as well as the format of the records:

Function:

- Administrative records (including, for example, personnel, estates, financial and accounting records, notes associated with complaint-handling)
- Patient health records (electronic or paper based, including those concerning all specialties and GP records)
- Accident & emergency, birth, and all other registers
- Theatre registers and minor operations (and other related) registers
- X-ray and imaging reports, output and images
- Records of private patients seen on NHS premises
- Integrated health and social care records
- Data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes.

This can include data for service management, research or for supporting commissioning decisions.

Format:

- Photographs, slides, and other images
- Microform (i.e. microfiche/microfilm)
- Audio and video tapes, cassettes, CD-ROM etc.
- E-mails
- Computerised records
- Scanned records
- Text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient) such as Twitter and Skype
- Websites and intranet sites that provide key information to patients and staff.

2.2 Records of NHS organisations are public records in accordance with Schedule 1 of the Public Records Act 1958. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. This applies regardless of the records format.

The guidelines in this Code apply to NHS records, including records of NHS patients treated on behalf of the NHS in the private healthcare sector and public health records, regardless of the media on which they are held. This includes records of staff, complaints, corporate records and any other records held in any format including both paper and digital records. The guidelines also apply to Adult Social Care records where these are integrated with NHS patient records.

See Information Governance Webpages for further details

2.3 The Trust must ensure that it adheres to all legislation and guidance in relation to Records Management. The Trust should:
Ensure there are strict guidelines in the formation of records and information, whether it is manual or computerised. See Information Governance Webpages for further details

-

Maintain, archive and track these records to ensure their use and validity. See Information Governance Webpages for further details

-

- Ensure all procedures and policies in relation to the completion of records are regularly updated and staff are suitably trained with new updates.

Store and preserve records in an environment where they are not susceptible to damage or destruction. See Information Governance Webpages for further details

-

Dispose of unwanted records, ensuring correct procedures are in place to uphold confidentiality. An unwanted record is classed as a record no longer required under retention guidelines. See Information Governance Webpages for further details

-
- Comply and ensure all Trust employees know the importance of security and confidentiality of information and records by offering training in all departments and services.
- Understand and comply with legislation and keep up to date on current issues relating to records management.

2.4 This document will provide guidelines for the creation, maintenance, archiving and disposal of records. All managers should ensure there are local procedures in place for staff to work in conjunction with this document. This guide highlights the need for accurate record keeping, the secure storage of records and the relevant disposal of records once they have exceeded their retention period.

Sections on accessing and transporting records are also included.

2.5 In addition to this policy, all clinical staff working for the trust should adhere to guidelines laid down by appropriate professional regulatory bodies.

2.6 This policy is mandatory for all staff working within the Acute Trust. **Persistent failure to comply with the requirements of this policy or a single incident of a serious nature, may lead to disciplinary action**.

3. Definitions

Records	Defined as 'information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of businesses. (ISO 15489:2001) Traditionally records were held on paper, or microfiche, but are now predominantly created and held in electronic format or within electronic systems.
Records	The above definition and qualities apply regardless of the record's format whether it is a sheet of paper, email, photograph or database entry. The retention of emails as records is a particular challenge.
Records Life Cycle	the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (for example closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation
Appraisal	Refers to the process of determining whether records are worthy of permanent archival preservation.
Records Management	A discipline which utilises an administrative system to direct or control the creation, version control, distribution, filing, retention, storage and disposal of records. This is done in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the Trust and preserving an appropriate historical record. The key components of Records Management are: □ Record Creation

		Record naming Filing structures/ File and folder referencing Tracking and tracing Retention and disposal, including appraisal
Metadata		Structure of records - Metadata makes it easier to manage or find information, be it in the form of webpages, electronic documents, paper files or databases and for metadata to be effective, it needs to be structured and consistent across organisations See Information Governance Webpages for further details

4. Responsibility and Duties

Shared Responsibility and Duties for NHS Records

All NHS records are public records under the terms of the Public Records Act 1958 S3(1)-(2). The Act sets out broad responsibilities for everyone who works with such records, and provides for guidance and supervision by the keeper of Public Records.

4.1 Statutory Responsibilities

The Secretary of State for Health, Strategic Health Authorities, NHS Trusts and other NHS bodies have a statutory duty to make arrangements for the safekeeping and eventual disposal of their records. The Trust is obliged to set out guidelines for creation, usage, storage and disposal of all records generated and received.

4.2 Managerial Accountability and Responsibility

The Chief Executive has overall accountability for the management of records within the Trust.

The Chief Executive is responsible for the retention of records and the Trust's Scheme of Delegation confirms this responsibility with the Chief Executive and the Director of Finance.

Line managers and supervisors must ensure that all staff are trained in the relevant aspect of record keeping dictated by their job role, and that there is compliance with Trust policies and procedures. This should be in the form of induction training internally by the line manager of the department. All departmental managers are responsible for regular, localised monitoring of the quality of documentation and adherence to this policy. In particular, managers and senior clerical staff should annually undertake a survey of the records for which they are responsible to ensure that the standards, as detailed in this policy, are maintained.

Line Managers should ensure that all staff undertakes Information Governance training at the appropriate level.

To further encourage integration of the management of risk throughout the Trust it is the responsibility of **all** staff to consider risks around Records Management and notify their line manager. Where appropriate, the issues will be identified within the Trust Risk Register and rectifying action taken.

Corporate records audit will be included in the annual Internal Audit programme every 3 years as requested by the information Governance Manager. See Information Governance Webpages for further details

4.3 Individual Responsibility

All employees are responsible for any records they may create or use. This responsibility is established and defined by the law. Any records created by employees are public records. They must ensure that the records are kept up-to-date and in good condition to have any real value to the Trust. Every person working for, or within the NHS, who records, uses stores or otherwise comes across information, has a personal common law duty of confidence as well as adhering to the Data Protection Act 1998. Personal information (e.g. about an employee or patient) processed or left for any purpose should not be kept for any longer than is necessary for that purpose and in line with the retention and disposal schedule. Patient/personal information may not be passed on to others without the person's consent except as permitted under Schedule 2 and 3 of the Data Protection Act 1998 or where applicable, under common law where there is an overriding public interest.

Under the Public Records Act 1958 employees are responsible for any records that they create or use in the course of their duties. Therefore, any records created or received by an employee of the NHS are public records and may be subject to both legal and professional obligations. For those records created in a local authority setting, such as adult social care and public health, section 224 of the Local Government Act 1972 applies as 'without prejudice to the powers of the custos rotulorum to give directions as to the documents of any county, a principal council shall make proper arrangements with respect to any documents that belong to or are in the custody of the council or any of their officers'.

Every employee's contract of employment clearly identifies individual responsibilities for compliance with information governance requirements – i.e. legislation, regulations, common law duties and professional codes of practice.

Employees should only access patient records where there is a clinical or business need to do so. Disciplinary action may be taken against individuals who access their own records or those of their friends, neighbours, colleagues, or any other person without authorisation.

4.4 Personal/Professional Integrity

All health care professionals have a legal duty of care; record keeping should be able to demonstrate:

- A full account of all assessments and the care planned and provided
- Relevant information about the condition of the patient or client at any given time and the measures taken to respond to their needs.
- Evidence that the duty of care has been understood and honoured and that all reasonable steps to care for the patient or client have been taken and that any actions or omissions have not compromised their safety in any way
- Professionals are accountable for ensuring that any duties, which they delegate to those members of the multi-disciplinary health care team who are not registered practitioners, are undertaken to a reasonable standard. For instance, if a professional delegates record keeping to pre-registration students or to assistants, they must ensure

that they are adequately supervised and that they are competent to perform the task and work to locally agreed protocols.

- In an inpatient setting, a registered person must clearly countersign any entry made by an unregistered person each day. In circumstances where a patient is receiving a regular, ongoing package of care and is being monitored by an unqualified member of staff, providing the patient's condition does not change, entries may be countersigned at a minimum of every six weeks. Entries made by unregistered staff should be checked and signed by registered staff to record a review and evaluation of patient care. An example entry may read " Ongoing care package reviewed today and previous entries by unqualified staff checked".
- Professionals are accountable for the consequences of entries made by unqualified members of staff.

4.5 Responsibilities of Third Parties

Where a non NHS agency or individual is contracted to carry out NHS functions, the contract must draw attention to obligations on confidentiality and to restrictions on the use of personal information, including those specified by the Data Protection Act 1998. The contract must require that patient information is treated and stored according to specified security standards, and is used only for purposes consistent with the terms of the contract. The contract should also make reference to the requirements laid out in the Freedom of Information Act 2000 (see Section 5.21). Action that will be taken in the event of confidence being breached (e.g. termination of contract) should be specified.

4.6 Responsibilities for Clinical Records

See the Clinical record keeping and records management Policy for information on clinical records

5. Policy Detail

Setting the NHS Standard

5.1 A systematic and planned approach to the management of records within the organisation, from the moment they are created to their ultimate disposal, ensures that the organisation can control both the quality and the quantity of the information that it generates: it can maintain the information in a manner that effectively services its needs, those of government and of the citizen: and it can dispose of the information efficiently when it is no longer required. This applies to all records whether manual or computerised records.

5.2 Records are valuable because of the information they contain and that information is only usable if it is correctly and legibly recorded in the first place, is then kept up to date, and is easily accessible when needed. Good record keeping ensures that:

- Employees work with maximum efficiency without having to waste time hunting for information.

- There is an 'audit trail', which enables any record entry to be traced to a named individual at a given date/time with the secure knowledge that all alterations can be similarly traced.
- New staff can see what has been done, or not done, and why.
- Any decisions made can be justified or reconsidered at a later date.
- Good records management is essential for:
- Providing high quality patient care
- Effective communication and dissemination of information between members of multi-disciplinary health care teams
- An accurate account of continuous assessment, treatment, and evaluation reflected in a care plan
- The ability to detect problems, such as changes in the patient's or client's condition, at an early stage
- Corporate memory
- Clinical liability
- Historical purposes
- Purchasing and contract service agreement management
- Financial accountability
- Disputes or legal action
- Continuity of care

5.3 It is therefore important to ensure:

- Important and relevant information is recorded and completed
- It is legible, written in black ink, and can be easily read and reproduced when required
- Information/records are easily accessible and kept up-to-date
- Information is shared rather than copied in order to reduce risks to confidentiality

Records are disposed of as soon as possible subject to national (Records Management Code of Practice for Health and Social Care 2016) or locally determined retention periods. See Information Governance Webpages for further details

-
- Records are shredded or disposed of via the Trust's contracts for disposal of confidential waste

5.4 What needs to be done to achieve best standards?

- Managers in all work units need to ensure that staff are aware of the current rules on such issues as Data Protection and access to patient information.
- Managers should ensure that staff are suitably trained in record keeping, security and storage of information/records (manual and computerised.)

5.5 Records may be required as evidence:

- Before a court of law
- The Health Service Commissioner
- In order to investigate a complaint at a local level
- By Professional Conduct Committees e.g. NMC, which considers complaints about professional misconduct

The main objectives of this policy are:

5.6 **Accountability** – that adequate records are maintained to account fully and transparently for all actions and decisions in particular:

- To protect legal and other rights of staff or those affected by these actions
- To facilitate audit or examination
- To provide credible and authoritative evidence

5.7 **Quality** – that records are complete and accurate and the information they contain is reliable and its authenticity can be guaranteed

Accessibility – those with a legitimate right of access can efficiently retrieve the information within them, for as long as the records are held by the Acute Trust. See Information Governance Webpages for further details

5.8

5.9 **Security** – that records will be secure from unauthorised or inadvertent alteration or erasure, that access and disclosure will be properly controlled and audit trails will track all use and changes. Records will be held in a robust format, which remains readable for as long as records are required

Retention and disposal – that there are consistent and documented retention and disposal procedures to include provision for permanent reservation of archival records See Information Governance Webpages for further details

5.10 **Training** – that all staff are made aware of their record-keeping responsibilities through generic and specific training programmes and guidance

5.11 **Performance measurement** – that the application of records management procedures are regularly monitored against agreed indicators and action taken to improve standards as necessary.

5.12 **Records Management - Scanning**

For reasons of business efficiency or in order to address problems with storage space, NHS organisations may consider the option of scanning into electronic format records which exist in paper format. Where this is proposed, the factors to be taken into account include:

The costs of the initial and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept;
The need to consult in advance with the local Place of Deposit or The National Archives (TNA) with regard to records which may have archival value, as the value may include the format in which it was created; and
The need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the Code of Practice for the Implementation of BS 10008 - Evidential Weight and Legal Admissibility of Information Stored Electronically
In order to fully realise the benefits of reduced storage requirements and business efficiency, organisations should consider disposing of paper records that have been copied into electronic format and stored in accordance with the appropriate standards.

Code of Practice for the Implementation of BS 10008 - Evidential Weight and Legal Admissibility of Information Stored Electronically.

The issue of Legal Admissibility is at the core of records management principles. An organisation must be able to prove (to a court of law or some other statutory body) that the contents of a particular document or data file created or existing within an Electronic Document Management System have not changed since the time of storage. If the data file is an electronically stored image of an original paper document, an organisation must be able to prove that the electronic image is a true representation of the original. Proving the authenticity of electronically stored documents is crucial to their admissibility in a court.

It is important for the system to be able to produce output that will ensure that a document is appropriately authenticated. The Code insists that the procedures and processes be audited annually, or more frequently for legally sensitive archives, to make sure that the approved procedures are being observed or that new ones meet the requirements of the Code and are formally and properly incorporated in the manual

5.13 Confidentiality and Security of Records

All NHS bodies and those carrying out functions on behalf of the NHS have a common law duty of confidentiality. Everyone working for or with the NHS who records, handles, stores or otherwise accesses patient information has a personal common law duty of confidence to patients/colleagues and to their employer. This duty of confidence continues after the death of the patient or after an employee or contractor has left the NHS. Trust staff are advised of their responsibilities on commencement of their employment and is reflected in their contracts.

The implementation of the Data Protection Act 1998 covers both computerised and manual personal data and establishes a set of principles with which users of personal information must comply. The Act also imposes statutory restrictions on the use of personal information, which must not be used for purposes other than those declared in the Trust's Data Protection Act registration.

The guidelines contained within this policy underpin the principles of the Data Protection Act and ensures that personal information is accurate, up to date and retrievable in a timely manner.

Through the Caldicott Guardian, Information Security and Information Governance Leads, the Trust must also ensure that information is shared "on a need to know" basis and that it is continuously improving confidentiality and security procedures governing access to and storage of clinical information. Paper records must be kept securely on Trust premises in a lockable filing cabinet.

Managers must ensure that all staff are made aware of their responsibilities regarding confidentiality and security of records. Support and guidance can be provided either by the trust's Caldicott Guardian, Security officer and the Information Governance Lead, or through the Information Governance Training Tool (e-learning facility) Contact the information governance manager for more information.

5.14 Electronic Records

Electronic information is subject to the same principles as paper records. For administrative records (e.g. minutes of meetings) these must comply with the principles laid out in this policy to aid effective storage and retrieval for responding to queries under the Freedom of Information Act.

Emails should be regarded as a transitory means of communication. Any information transmitted by email which falls into a category shown in the retention schedule should be absorbed into a mainstream filing system which is subject to the requirements laid out in section 5 "Record Keeping Standards".

As an example a Word attachment containing minutes of a meeting should be stored in either the electronic or manual filing system of the person sending the email. Neither the sender nor recipient should save the email, with the attachment, in perpetuity. For this same reason any information sent by email which is intended to have some permanence should be transmitted as a file attachment and is subject to the above conditions.

5.15 Freedom of Information Act 2000 (FOI)

- The Freedom of Information Act was passed on 30th November 2000 and is part of the Government's commitment to greater openness in the public sector.
- On 1st January 2005, the Act gave a general right of access to all types of 'recorded information' held by public authorities, subject to certain conditions and exemptions contained in the Act.
- Simply, any person of any nationality, who makes a request to a public authority for information, must be informed whether the public authority holds the information and if so, that information must be supplied. This is referred to as the 'duty to confirm or deny'.

5.16 FOI Publication Scheme

- In addition to providing information when asked to do so, the Act also requires public authorities to be proactive in the release of official information.
- As a result, by 31st October 2003, every public authority was required to adopt and maintain a publication scheme setting out how it intends to publish the different classes of information it holds, and whether there is to be a charge for the information disclosed. The trust's FOI publication scheme is regularly updated and has been approved by the Information Commissioner.
- The Trust's FOI Publication Scheme can be found on the trusts internet site.
- Freedom of Information Act 2000 Policy
- The trust's FOI Act 2000 Policy provides a framework within which the trust will ensure compliance with the requirements of the Act. It is not a statement of how compliance will be achieved; this will be a matter for operational procedures.
- The Policy will underpin any operational procedures and activities connected with the implementation of the Act.
- The FOI Act 2000 Policy applies to all trust employees and to non-executive directors.
- The Freedom of Information Act does not overturn the common law duties of confidence nor does it overturn the requirements of the Data Protection Act 1998.

6. Implementation

6.1 Plan for implementation

The Information Governance Manager will ensure that this policy is sent to all directorate managers within the Trust. It is then their responsibility to ensure that all staff groups within their area are directed to this policy. Workshops on Information Governance and the importance of records management will be held regularly and departmental visits within the Trust by the Information Governance Team will highlight this policy and ensure that it is being followed. After each departmental visit, all records that are being held (both manual and electronic) will be logged on the central records inventory log held by the Information Governance Manager. Any staff who control records kept in the area will be asked to contact the IG department if changes occur with the records they hold.

6.2 Dissemination

This policy will be available on the Trust Intranet. A notice board link will be sent out to all acute staff via email. The Head of Information/Information Governance Manager will send the link to this policy to all Directorate managers and ask that it is disseminated to all staff groups. Each departmental visit will ensure that appropriate staff are aware of the policy.

6.3 Training and awareness

The data security awareness online training is provided by NHS digital via ESR and all staff must completed this training on an annual basis. There is a paper version which reflects the online version provided for ancillary staff.

7. Monitoring and compliance

See the table below for monitoring

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?**
Page 6 4.2	All departmental records must be added to a corporate records management survey sheet	Managers and senior clerical staff should annually undertake a survey of the records for which they are responsible to ensure that the standards, as detailed in this policy, are maintained.	Annually	Information Governance Officer/Manager	IGSG (monitored via the IG work plan)	Ad Hoc
Page 6 4.2	Corporate Records Audit	Records Audit	Every 3 years	External Audit	Information Governance Steering Group	Following audit

8. Policy Review

This policy has been developed to ensure that the Acute Trust has an internal policy that clearly shows the correct protocol for all records management within the trust. The Information Governance Manager will ensure that any new legislation and guidance from The Department of Health and NHS Information Authority will be reflected in this policy and disseminated throughout the Trust if changes are made prior to the next revision of the policy

This policy will be reviewed in 2 years (See details of next review on title page) by the Information Governance Steering Group and the Key Documents Approval Group

9. References

References:	Code:
Data Protection Act 1998	
Freedom of Information Act 2000	
Clinical Health Records Management Policy	
Incident Reporting Policy (in regards to records)	
Claims Handling Policy and Procedure (in regards to records)	

10. Background

10.1 Equality requirements

None - equality assessment Supporting Document 1

10.2 Financial risk assessment

None - financial risk assessment Supporting Document 2

10.3 Consultation

The policy has been updated by the Information Governance Manager with input from the Information Governance Steering Group members. It has been created in line with national requirements set out in Records Management Code of Practice for Health and Social Care 2016.

Contribution List

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

Designation
Director of Resources/SIRO (Chair)
Director of Asset Management and ICT
Information Governance Manager
Information Governance Officer
Head of Human Resources - Workforce
Deputy Director of Nursing
Head of Legal Services
IT Operations Manager (on behalf of WHITS Director of IT)

Head of Risk Management and Clinical Governance
Chief Medical Officer – Caldicott Guardian
Company Secretary

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

Committee
Information Governance Steering Group

10.4 Approval Process

This policy will be approved by the Key Documents Approval Group bi-annually.

10.5 Version Control

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

Date	Amendment	By:
April 2009	Updated in to Trust policy format	Information Governance Manager
April 2009	Updated to include changes to national requirements	Information Governance Manager
Dec 2011	Updated into new Trust policy format. including minor updates to reflect national requirements	Information Governance Manager
April 2014	Updated into new Trust policy format. including minor updates to reflect national requirements	Information Governance Manager
May 2017	Updated – see amendments box on page 1	Information Governance Manager
May 2019	Minor update including, relevant dates and approval Appendices removed and available on the Information Governance Webpages	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?**	No	
6.	**What alternatives are there to achieving the Policy/guidance without the impact?**	No	
7.	**Can we reduce the impact by taking different action?**	No	

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:	None

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