Trust Policy	Worcestershire Acute Hospitals NHS Trust

Corporate Records Management Policy and Procedure

Department / Service:	Corporate
Originator:	Information Governance Manager
Accountable Director:	Director of Finance (SIRO)
Approved by:	Information Governance Steering Group (IGSG) Key Documents Approval Group (KDAG)
Date of approval:	25th May 2017 at Information Governance Steering Group 25th July at Key Documents Approval Group
First Revision Due:	25th May 2019
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:

Definitions updated
Sections 1.3, 2.2, 4.3 now include a reference to the Public Records Act 1958
Section 1.6 has additional statutory and NHS guidelines:

- Records Management Code of Practice for Health and Social Care 2016
- Information Security Management: NHS Code of Practice
- Standards for the clinical structure and content of patient records
- Independent Inquiry into Child Sexual Abuse (IICSA),

Section 2.1 now has reference to ISO standard, ISO 15489-1:2016 Information and documentation
Section 2.1 has a wording update to the function and format definitions
Removal of specific clinical record information as this is incorporated in the Clinical record keeping and records management Policy, including the auditing/monitoring of clinical records
Section 10.3 - Contribution list to include all IGSG current members
Further guidance on the following subjects included as additional appendices:

- Declaring a record
- Records metadata
- Appendix 12 - Updated Retention and Disposal Schedule. The schedule has

reduced from 101 pages down to 30. The main repercussion is likely to involve IG staff providing advice to staff when the specific document is not listed and advice as to the nearest category.

- Storage of records
- Specific types of records

Contents page:

Appendices

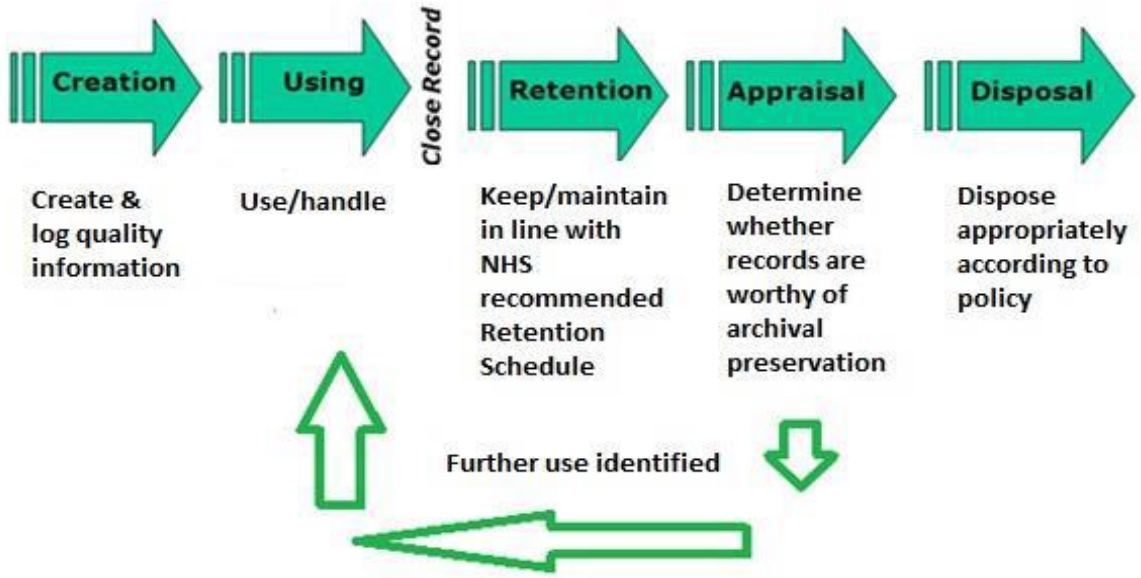
Supporting Documents

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 appendix 1 – declaring a record)
(See appendix 11 – Specific types of records guidance)

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 appendix 3 – standards)
- Maintain, archive and track these records to ensure their use and validity. (see appendix 4 – tracking)
- 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 appendix 5– storage standards)
- 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 appendix 8 – appraisal and destruction)

- 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 Appendix 2)

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 appendix 13 for an example of the trusts corporate records inventory form)

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 **Appendix 12** for link to the schedule)
- 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

5.8 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 Appendix 6 – records storage and retrieval)

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

5.10 Retention and disposal – that there are consistent and documented retention and disposal procedures to include provision for permanent reservation of archival records (see appendix 7 – continued retention)

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

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

5.13 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

5.14 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.

5.15 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.

5.16 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’.

5.17 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

All departmental managers are responsible for ensuring that relevant staff attend training in records management, case note handling and confidentiality.

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

Declaring a Record

Within the record keeping system, there must be a method of deciding 'what is a record?' and therefore 'what needs to be kept?' This process is described as 'declaring a record'. A declared record is then managed in a way that will hold it in an accessible format until it is appraised for further value or it is destroyed, according to retention policy that has been adopted.

Some activity will be predefined as a record that needs to be kept, such as clinical records. Other records will need to fulfil criteria as being worth keeping, such as unique instances of a business document or email. Key legislation, such as the DPA or FOIA, applies to all recorded information of the types covered by these Acts, whether declared as a formal record or not.

Declaration makes it easier to manage information in accordance with the legislation and business need. Accumulations of informal recorded information should be minimised as they will rarely meet these requirements.

A record can be declared at the point it is created or it can be declared at a later date, but the process of declaring a record must be clear to staff.

Declared records can be held in the 'business as usual' systems or they can be moved into a protected area, such as an EDRMS, dependant on the record keeping system in use.
It is harder to manage records over their lifecycle if they clutter up the folders or the workspace used on a daily basis or they are held in personal systems where only one person can access them. Just as a paper file was once closed when full or it ran over into the following year's business cycle, electronic information must also be closed off and filed in a place that does not clutter up the current business.

This declared information can be moved into the appropriate part of the business classification scheme, if it does not already reside there, following creation. The individual staff and teams have the flexibility to apply the organisational policy to keep the records for the appropriate length of time in their business context. This system, while flexible, runs the risk of staff and teams not applying the policy correctly and records may be missed.

Records and Metadata

Record keeping systems must have a means of physically arranging or organising records. This is often referred to as a file plan or by the technical name of a business classification scheme. The scheme can be designed along several lines:

- Function (recommended)
- Hierarchy/organisation
- Hybrid function/hierarchy
- Subject/thematic

The scheme will enable appropriate management controls to be applied and support more accurate retrieval of information from record systems. When the recommended functional classification has been selected, the scheme can be further refined to produce a classification tree based on function, activity and transaction.
Function-Activity-Transaction
Classification schemes should try and follow the rule of classifying by function then by the activity and finally the transactions that relate to the activity. The transaction can then be assigned a rule (such as retention period) a security status or other action based on the organisational policy.
At the simplest level, the business classification scheme can be anything from an arrangement of files and folders on a network to an Electronic Document and Records Management System (EDRMS). The important element is that there is an organised naming convention which is logical and can be followed by all staff.

Metadata Standard

The Cabinet Office e-Government Metadata Standard v3.1 2006 states that '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'. There are 25 metadata elements which are designed to form the basis for the description of all information. The standard lists four mandatory elements of metadata that have to be present for any piece of information. A further three elements are mandatory if applicable and two more are recommended. These can be found in Table A

Table A – Metadata elements

Mandatory elements	Mandatory if applicable	Recommended
Creator	Accessibility	Coverage
Date	Identifier	Language
Subject	Publisher	
Title		

An example in practice of a box label on the side of a box of records would be created as shown in Table B
.

Table B – An example of the use of the metadata standard

Box label	Local interpretation	Metadata standard
Tiverton Community NHS Trust	Organisation Name	Creator
Midwifery	Service Name	Creator
Patient case records surname A-F	Description of record	Subject/Title
2000	Date/year of discharge	Date
2025	Date/year of destruction	Date

In addition to any metadata needed to manage information through the lifecycle, all information possesses a security classification.

Both central government and local government use the Cabinet Office Government Security Classifications April 2014 defined protective marking scheme. This policy describes how HM Government classifies information assets to: ensure they are appropriately protected; support public sector business and the effective exploitation of information. The policy also describes how government can meet the requirements of relevant legislation and international/bilateral agreements and obligations. It applies to all information that government collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners.

The NHS use a variation of this scheme based on patient data being classed as 'NHS Confidential' having the equivalence of Official Sensitive under the 2014 scheme.
Where a record has enough metadata it can be managed through the lifecycle, possess a security classification and be easily found if needed.

More information about metadata elements and the Cabinet Office e-Government Metadata Standard 2006, including a full description of the 25 elements, can be found on the National Archives website.

Metadata only Classification

If a record has sufficient metadata, the arrangement between itself and other records in the same class can be established without the application of a business classification scheme. At present, ISO 15489 and the 'Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 200039' calls for records to be arranged into a classification scheme.

Records that are not stored or arranged in logical filing systems often lack their characteristic of 'context' which will reduce the ability to produce an authentic record. They are often reliant on a powerful search tool used to 'mine' the data or use a process called 'digital archaeology'. This records management method is not recommended because it is so time-consuming to determine authenticity but it has been included in this Code as legacy record keeping systems may not have been organised logically.

As record keeping systems are updated and the more traditional files and folders and bespoke storage for electronic records are decommissioned, the ability to recover records is only as good as the metadata applied to records when they were created.

Business Classification Scheme Design

The technical name for the process to create business classification system is 'functional decomposition'. In the most basic form this is a list of activities arranged by business functions; however it is often linked to organisations hierarchical structure. An example is given in Table C.

Table 6 - Business Classification Scheme Design

Functional classification example	Hierarchical classification example
Finance-Accounts-Payments-HR Payments (Note All payments including HR team are recorded under the activity of accounts)	Finance team-Accounts Team-Payments HR Team – Finance- Payments (Note The payment is recorded twice)

Good Practice for business classification scheme design:
The NHS Business Services Authority has devised a business classification scheme that allows it to manage records so they can be easily found and managed through the lifecycle. Each record can be assigned a retention period once it is declared into the system.
http://www.nhsbsa.nhs.uk/Documents/NHSBSACorporatePoliciesandProcedures/NHSBSARM014_Business_Classification_v1.0_2011.pdf

RECORD KEEPING STANDARDS

A record is a structured document which contains information, (in any form of media), which has been created or gathered as a result of any aspect of the work of the NHS employees. These records must be continually updated to ensure their validity and use, unless the information contained in the record becomes obsolete.

Creating Records

All records should have a unique number or filing system, which will be applicable only to that record. For example:

- A patient's medical record will be identifiable by the patient's Unit Number.
- An employee's electronic personal record identified by a personal number.

All records must have clear and precise formats.

They must be structured in the same way that files of the same description are structured with an easy to follow standardised index, so that information can be retrieved quickly and easily (for example all patient and employee files). In respect of other information and records, they should be kept in some sort of indexed format either numerical, by date or alphabetically.

Managers should ensure that this is the practice within their own departments and relevant guidance is in place.

Updating Records

- Managers should ensure that all records should be regularly updated and maintained in a practical order.
- Great care should also be taken when storing these files, to ensure their safety and safekeeping.
- Records which are no longer required should be considered for archiving or disposal, depending on their recommended retention period.
- For paper records, regular checks on the status of the record container, whether it is a binder, paper folder or box file, should be undertaken to ensure no damage has occurred, or if it has to replace it quickly before it is further damaged.
- Concise and easy to follow procedures, whether they are paper or electronic systems, should back up all record keeping practices.
- Managers should ensure all staff are correctly trained. Further advice about training can be sought from the IT training Department for the Trust.

Documentation of Record Systems, Manual and Electronic

The following should be documented when a file is created:

- File reference
- File title
- Protective marking, i.e. Restricted, Confidential, Secret or Top Secret
- If possible an anticipated disposal date and what action to take
- Where action cannot be anticipated, mechanisms must be in place to ensure this action takes place when the file is closed
- All filing systems should be documented and kept up-to-date

The following list includes some of the basic standards expected in relation to **clinical** record keeping. Please refer to the trust's Clinical Record Keeping Guidelines for full guidance:

Date and time

All entries should be dated and timed. It is essential for a clinical record to have both.

Creator of the Record

The creator of the record should be clearly identified. The person's name and designation should be printed. A clearly recognisable signature should accompany all clinical notes, financial records and letters and documents.

Abbreviations

Abbreviations should be avoided wherever possible. Where possible, the full meaning of an abbreviation should be cited the first time it is used. NB For patient records, abbreviations are not approved by professional bodies and should be avoided.

Alterations

Do not try to hide errors. Paper records should have errors scored out with a single line and be initialled, dated and timed. Electronic records should have audit trails.

Additions

If an addition needs to be made to a record it should be prefaced with a comment indicating that this is an additional or late entry and be separately dated, timed and signed. Never try to insert notes, especially after notification of a complaint or claim. Never try to disguise additions to a record.

Personal Comments

Only include commentary that is relevant and appropriate to the record. Records are not the place to note offensive observations about a person's character, appearance or habits. Under the Data Protection Act 1998, members of the public are allowed to have access and view the content of their records. Offensive, personal or humorous comments about an individual must not be recorded.

Dictated Notes

Typed notes must be checked and signed by the professional who dictates them. Responsibility for the accuracy of the record lies with the person who created the record not the typist.

Completeness

A record needs to contain sufficient information to be fit for purpose, factual, consistent and accurate. Standard request forms e.g. test results or order forms should be complete. Insufficient information may lead to serious mistakes.

All patient records must be written contemporaneously - 'As soon as possible after contact and within the same working day', although a record made within twenty-four hours of the event to which it relates would suffice (DOH 1990).

Reports

Reports need to be evaluated by the appropriate professional and any action taken documented within the record.

Clarity and Legibility

Records need to be clear and legible. A hand written record should be written in permanent black ink wherever possible. This will give the records greater clarity and legibility when photocopied. If it is not possible for a person to write legibly, then the record should be typed. Thermal faxes may fade and should not be included as part of a permanent record. The information should either be transcribed into the record, the original requested or an indelible photocopy made of the fax.

In addition, records must:

- be written, wherever possible, with the involvement of the patient or client or their carer (ensuring patient confidentiality is maintained)
- be written in terms as far as possible that the patient or client can understand
- be consecutive
- provide clear evidence of the care planned, the decisions made, the care delivered and the information shared

Using Records and Records Tracking Systems

1. Accurate recording and knowledge of the whereabouts of all records is essential if the information they contain is to be located quickly and efficiently. One of the main reasons why records get misplaced or lost is because their next destination is not recorded anywhere.

2. A tracking system for all records should be in place to ensure that all information can be found quickly and easily. The tracking system could be a manual one i.e. the schedule of Trust's policies identifies the policy number for a certain issue, or computerised and linked to a department's IT system i.e. PAS note tracking system.
3. A manual tracking system may consist of a book, diary or index card to record movement of information an electronic tracking system could be on excel spread sheet or a database held on computer. To ensure that information is correct and applicable, all departments must ensure that their tracking system is routinely checked and updated.
4. Tracking systems should record the following (minimum) information
    - The reference number of the record
    - Any other applicable identifier i.e. department, hospital or ward code
    - Person, unit, department or place to where it is being sent
    - Date of transfer
    - Date of information being received back (if applicable)
5. Managers should ensure that procedure notes and training are in place to maintain and regularly update the tracking system.
6. Managers should also ensure any tracking system is stored securely and access should only be given when applicable.

Storage

Paper: to establish the authenticity of paper records and to meet the Care Records Guarantee that the service user can see who has accessed their records, the records must be held according to the standard that allows access to be audited.

The current guidance to identify and support the requirements for offsite storage of physical records is issued by TNA40. The standard issued by TNA (Tracking Records – RMS 2.141) is a best practice benchmark for all organisations creating or holding public records. The standard provides advice and guidance on the tracking of records at all stages of the information life cycle up to destruction, or transfer to TNA or an approved place of deposit.

Digital: digital information must be stored in such a way that throughout the lifecycle it can be recovered in an accessible format in addition to providing information about those who have accessed the record, as required by the Care Records Guarantees. When considering standards, the European Commission DLM Forum Foundation 'Modular Requirements for Record Systems' is frequently used as the overarching standard.

The authenticity of a record is dependent on a number of factors not least that it has sufficient metadata to allow it to remain reliable, integral and usable. This will include the structure of the record, the business context and links between other documents that form part of the transaction the record relates to.

It should not be underestimated how technically difficult and time consuming this process can be to maintain digital records over time. A record with web links that do not work once they are converted to another format loses integrity. A record with attachments, such as hyperlinks or embedded documents, that do not migrate cannot be said to be integral. An email message that is not stored with the other records related to the transaction is not integral as there are no supporting records to give it context.

Offsite: It is vital to highlight the importance of actively managing records which are stored in offsite storage. This will ensure that the organisation maintains a full inventory of what is held offsite, retention periods are applied to each record, a disposal log is kept, and privacy impact assessments are conducted on the offsite storage providers.

Records Storage, Retrieval and Access

The Trust has a responsibility for ensuring the effective and efficient operation of all storage facilities within the organisation. This includes the safekeeping, accessibility and retention of records for as long as required, the transfer of those records selected for permanent preservation, and the timely destruction of records no longer required. Storage should also be in a suitable environment, which has easy access and appropriate safety to ensure the records are not damaged or destroyed. All records storage areas should meet with Health and Safety requirements.

1. Shelving and boxing

- Records should be stored on shelves or in cabinets in a way which facilitates easy and safe retrieval. This will not only provide for access to the records but will also make security checks more effective.
- Paper records need not be boxed, although boxing may be required where, for example, there are risks from damage by excessive light or by flooding, or where there is a high probability that certain records will be selected for permanent preservation.
- Film should be stored in dust-free metal cans and placed horizontally on metal shelves. Microform, sound recordings and video tape should be stored in metal, cardboard or inert plastic containers, and placed vertically on metal shelving, where appropriate.
- Computer disks and tapes should be stored in durable boxes not susceptible to mould, damp or water.
- Ideally computer, media and microfilm/fiche should be kept in a fireproof safe.
- Records should be stored off the floor to provide some protection from flood, dampness and dust.
- The width of aisles and general layout of storage areas must conform to fire, health and safety, and similar regulations.
- Large documents, such as maps, should be housed in special storage equipment to ensure that they are not damaged and are readily accessible.
- Old X-rays should be kept by the X-ray Department and according to local procedures.

2. Protection against fire and water

- All storage facilities should be protected by an automatic fire detection and alarm system including smoke detectors, installed and maintained.
- Portable fire extinguishers should be provided and should be installed at various points within the storage areas.
- Staff should be instructed in the location and use of firefighting equipment, and fire drills should be undertaken.
- Records should not be stored where there may be a danger of flooding from pipes or radiators.

3. Environment

- Unsuitable environments may cause irreversible damage to records than any other factor.
- Managers must check humidity and ventilation within storage areas.

- Regular maintenance of heating and ventilation systems is essential.
- Managers must ensure fluctuations in temperature are monitored as they may cause significant damage to the records, whether paper format or other media.
- If the humidity within the storage area rises at any time, there is a great risk of mold growth. Managers must prevent this as damage could be irreversible to paper, microfilm/fiche or computer media.

4. Transportation of records

All records must be safeguarded from theft, damage or destruction. If a person's job role includes the transferring of records or using them at meetings the following guidelines must be adhered to.

By vehicle

- Records should not be left unattended in the vehicle.
- They should not be left unattended at any location, unless in a locked facility.
- The person using the record at the time is responsible for their safekeeping.
- No one else in the vehicle should access the records unless they are authorized to.

By post

- Records sent by post/porters should be carefully packaged to ensure they are not damaged when transported.
- They should be clearly labelled to the addressee.
- If they are to be delivered by the porters, then the porters should be given precise details of their destination.
- All records being transported externally must be sent recorded delivery, to ensure a record of their journey is available, in the event that they go missing.
- It must be noted on the record tracking system that the records have left their normal storage.

5. By electronic means:

Email

Records sent by email must be undertaken in line with the Countywide Internet/Email Policy and the Trust's Code of Conduct for Employees in Respect of Confidentiality. (refer to Trust intranet site)

Fax

Transmission of records by fax may be carried out routinely if the recipient machine is known to be a safe haven / secure fax and the sender confirms that the correct number has been dialled. (refer to Safe Haven Policy on intranet)
Transmission of records by fax to a machine that is not a safe haven / secure fax may be carried out provided the following precautions are taken:

- Telephone the recipient to forewarn of the transmission and to confirm the number
- Use pre-programmed numbers wherever possible
- Request that the recipient waits by the machine to receive the transmission
- Request that the recipient confirms receipt by telephone

- Ensure that there is a cover sheet that clearly states who the information is for and mark it “Private and Confidential”
- Check the recipient’s number again before transmission
- Where possible, obtain a report print out from the machine to confirm successful transmission

Keeping patient records at home:

Where it is not possible to return records to a trust base at the end of a working day it will be permissible for records to be held overnight by staff in their homes. During this time it is the member of staffs responsibility to ensure records are secure, made available to the trust if required and their confidentiality maintained at all times.

Under no circumstances should records be left in staff vehicles overnight or when such vehicles are left unattended for extended periods – this includes staff diaries.

ACCESS TO RECORDS

Levels of confidentiality bind all employees. Managers must ensure that all staff are trained in data protection and are aware of the implications if confidentiality is breached. The impact of a breach of confidentiality could be any of the following:

- Threat to personal safety or privacy
- Embarrassment for the Trust and NHS
- Legal obligation or penalty
- Financial loss
- Disruption of activities

The Trust is committed to multi-disciplinary working procedures and this requires all key professionals to work together and share information, to the benefit of the patient/client. Patients/clients have an expectation that information held relating to them is confidential and held securely.

Review for Continued Retention

The periods given in the schedules to this Code are the **minimum** periods for which records must be retained for NHS business and clinical purposes. In most cases, it will be appropriate to destroy records immediately once this period has expired, unless they have been selected for transfer under the Public Records Act 1958. If personal data is held for longer than necessary it may breach principle five of the DPA.

Organisations must have procedures and policies for any instances where it is necessary to maintain records for longer than the stated minimum, including temporary retention where records due for destruction are required to support reasonably foreseeable litigation, public inquiries, an on-going FOI request or similar exceptional statutory reasons, such as a public inquiry.

Organisations may also set local policies, for example for retention of clinical records in relation to specific circumstances beyond those identified in this Code.

Where records contain personal data, the decision to retain must comply with the DPA principles.

Decisions for continued retention beyond the periods laid out in this Code must be recorded, made in accordance with formal policies and procedures by authorised staff and set a specific period for further review.

Records **may** be retained beyond the statutory period (20 years from the last date at which content was added) set by the Public Records Act 1958 **only** with the approval of the Secretary of State for Culture, Media and Sport. Applications for approval should be made to TNA in the first instance.

Retention Instrument 122 has been approved by the Secretary of State for Culture, Media and Sport to permit extended retention of NHS individual staff and patient records where this is mandated by this Code or is otherwise necessary for continued NHS operational use. Where organisations use the provisions of the Instrument to extend retention, this must be documented in published policies. TNA website has details of those currently in force.

Transfer to a Place of Deposit

The Public Records Act 1958 requires organisations to select core records for permanent preservation at the relevant Place of Deposit (PoD) appointed by the Secretary of State for Culture, Media and Sport. PoDs are usually public archive services provided by the relevant local authority.

The selection and transfer must take place at or before records are 20 years old and is a separate process from appraisal for retention to support current service provision. Potential transfers of digital records should be discussed with the PoD in advance to ensure that technical issues can be resolved.

Records no longer required for current service provision may be temporarily retained pending transfer to a PoD and records containing sensitive personal data should not normally be transferred early.

Transferred records should be in good condition and appropriately packed, listed and reviewed for any FOIA exemptions. For more detail on the transfer process and sensitivity review, see the TNA guidance on their website.

More detailed guidance on the selection for records for transfer under the Public Records Act 1958 is contained in the schedules to this Code. The relevant PoD will provide additional local guidance on how the schedules should be implemented. Current contact details of PoDs and the organisations which should transfer to them can be found on the TNA website. As a general rule national public sector organisations will deposit with TNA while local organisations will deposit with a local PoD.

Selection of NHS Records for Permanent Preservation

All NHS records are public records under the terms of the Public Record Act 1958. Records over thirty years old and selected for preservation will be stored at a designated Local Authority Record Office which has been authorized by the Public Records Office unless other arrangements have been made by the Trust.

Permanent preservation at Local Authority Records Office

- The retention and disposal schedule highlights records suggested for permanent preservation.
- Departmental managers must identify which records they wish to preserve.
- Arrangements then should be made with the Local Authority Records office for the transporting and storage of the records.
- A list should be made of all records sent for preservation.
- This includes records of paper, microfiche/ film and computer media.
- Access to the records will only be available through an arrangement with the Local Authority Records office.

Permanent preservation by electronic media.

- Managers may decide that they wish to retain copies of records in electronic format.
- If this is the case the manager should contact the Head of IT to investigate the use of record scanning.
- The records will be fed through a scanner and the image of the record will appear on the screen.
- Once quality checks have been made, the record is then linked to an identifier.
- The record will either be stored on disk or on a computer network.
- The records can then be disposed of as per Section 11. A list of these records must be kept for future reference.
- Managers may want to consider this approach, as it will free up storage space for more current records.
- This process will be beneficial to all types of records held by the Trust.

Archiving Records

When a record reaches the end of its retention period or there is a lack of sufficient storage facilities, the Departmental Manager using national and local guidance from the Retention and Disposal Schedule should consider whether the record should be destroyed or could be sent for secure archiving off site.

Only approved suppliers can be selected and managers should refer to the Trusts storage contact arranged by HPC/Supplies.

Once a decision has been made that a record is to be archived off site, then the departmental manager should follow this procedure: -

- A list of all the records that are to be archived must be taken and kept indefinitely for audit purposes (See **Appendix 10 – archiving of records form**)
- The Departmental Manager should access the trust contracted archive facility to store the records off site securely.
- The Departmental Manager should ensure that the contract with the archive company includes a confidentiality clause, which ensures the archive company adheres to the Data Protection Act 1998 and the common law duty of confidentiality
- The records should ideally be filed chronologically and in alphabetical order. The department and the name of the team (where applicable) should be written on the box
- The department and senior manager must sign the list to confirm the archiving of the records and the details for future reference by the Trust and Audit

Retrieval and / or Access

- Any accesses to the records should be recorded to detail the date of access, details of the person and the reason access was required
- If records are taken away from the archive a receipt should be obtained from the taker of the record, this should be recorded and when the record is returned this should also be recorded.

Please refer to Appendix 10 for further details on archiving and retrieval of records.

Regular archiving should take place for both manual and electronic records.

The 20 Year Rule for the NHS – records of local interest

In July 2012 the Government announced that from 1 January 2013, central government departments would begin transferring records in line with the new 20-year rule. This replaces the previous 30-year rule, and the change means that thousands of historical records will be released to the public much earlier than previously possible. To assist this process, additional information on corporate records management for NHS Acute, Ambulance, Community and Mental Health Trusts was collected with version 11.2 of the IG Toolkit, in December 2013

Design and Implementation of Record Keeping Systems (DIRKS) – please access the Records Management Code of Practice for Health and Social care for further information on DIRKS

Appraisal

The process of deciding what to do with records when their business use has ceased is called appraisal. This must be defined in a policy and any decisions must be auditable and linked to a mandate to act, derived from the Board. No record or series can be automatically destroyed or deleted. It is good practice to get authorisation for deletion or destruction from an appointed committee or group with a designated function to appraise working to a policy or guidelines. There is some guidance from TNA on appraisal.
There will be one of three outcomes from appraisal:

- Destroy / delete
- To keep for a longer period
- To transfer to a place of deposit appointed under the Public Records Act 1958.

The retention schedule included in this Code lists those records which should or may be selected for transfer to a place of deposit. There are also a number of other records which may be of interest to a local place of deposit. Appraisal may also result in a record being retained for longer. If as a result of appraisal, a decision is made to destroy a record there must be evidence of the decision.
Records selected as a result of an appraisal may also have security classifications applied which may continue to exempt them from Freedom of Information (FOI) requests or disclosure after transfer to a place of deposit. This may be part of the annual cycle of the records committee or other appropriate person where a record will be retained in an official document such as committee papers. Records transferred to a place of deposit, such as unpublished board papers, may continue to be subject to FOI Act exemptions on public access following transfer.
Electronic records can be appraised if they are arranged in an organised filing system which can differentiate the year the records were created and the subject of the record. If electronic records have been organised in an effective file plan or an electronic record keeping system, this process will be made much easier. Decisions can then be applied to an entire class of records rather than reviewing each record in turn.

Destruction

Paper: paper records can be destroyed to an international standard. They can be incinerated, pulped or shredded (using a cross cut shredder) under confidential conditions. Do not use the domestic waste or put them on a rubbish tip, because they remain accessible to anyone who finds them. The relevant standard for destruction in all formats is the British Standard IA EN15713:2009 - Secure Destruction of Confidential Material.
As referenced in the retention schedule, it is important to keep accurate records of destruction and appraisal decisions. Destruction implies a permanent action. For electronic records ‘deletion’ may be reversed and may not meet the standard as the information can/may be able to be recovered or reversed.
Digital media: destruction of digital information is more challenging. Records management is concerned with accounting for information so any destruction of hard assets, like computers and hard drives and backup tapes, must be auditable in respect of the information they hold. An electronic records management system will retain a metadata stub which will show what has been destroyed.
The Information Commissioners Office (ICO) has indicated that if information is deleted from a live environment and cannot be readily accessed then this will suffice to remove information for the purposes of the Data Protection Act. Their advice is to only procure systems that will allow permanent deletion of records to allow compliance with the law.

Please contact the NHS Digital for procurement advice and example documentation for procurement of information systems that support the requirements for care record systems. Requests made to organisations under the FOI Act have indicated that once the appropriate limit for costs incurred for that FOI has been reached, there are no more requirements to recover information held. This will **not** apply if a court has instructed information to be destroyed where permanent destruction will be required, including all copies and instances of the information.

At present there are two ways of permanently destroying digital information and these are either: overwriting the media a sufficient number of times or the physical destruction of the media.
No information can be destroyed if it is the subject of a request under the DPA and/or FOIA or any other legal process, such as an inquest following a death.

Disposal of Records

The length of the retention period depends upon the type of record and its importance to the business of the Trust. The Department of Health has issued the NHS Code of Practice in Records Management, which gives guidance on the retention and disposal of records. There may be additions to or deletions from the schedule to suit the needs of the Trust.

Process for disposal

Each department that holds any records should have a tracking system, which identifies all records, their date of creation, and where they are stored.

It is therefore the responsibility of the departmental manager or their deputy to identify the records, which can be destroyed. Refer to the Retention and Disposal Schedule

Once the records have been identified, then the decision should be made by the relevant senior manager in discussion with the department manager whether:

- Paper records should ideally be scanned into electronic format and then destroyed. This would apply to all medical and personnel records.
- Records preserved forever in their original format.
- Records are destroyed completely.

The scanning option may be beneficial in some cases as the destruction of paper records is irreversible and cannot be rectified later.

Once the records have been scanned or the decision was made to destroy them then the manager should follow this procedure:-

- A list of all disposed records must be taken and kept indefinitely for audit purposes. (See **Appendix 9 – disposal form**)
- The Estates Department will have a contract with a reputable disposal firm to destroy the records by pulping or incineration.
- The Supplies Manager should ensure that the contract with the disposal company includes a confidentiality clause, which ensures the Trust adheres to the Data Protection Act 1998 and common law.
- The records should be shredded (not including Medical records) and placed in appropriate bags for collection by the company.

- The department and senior manager must sign the list (**Appendix 9**) to confirm the destruction of the records and the details of the disposal for future reference by the Trust and Audit.

Destruction of Records and the Freedom of Information Act 2000

It is an offence to destroy files with the intention of preventing their disclosure once a request to see them has been made under the Act.

If information has been deleted or destroyed under the Retention and Disposal Schedule of this Policy, the applicant will need to be informed, with a justification for destruction.

If a record has been disposed of legitimately in accordance with this policy, it is not liable to disclosure under FOI. However, where a record is retained it remains liable to disclosure whether or not the minimum retention period has passed.

If the information requested is due for destruction within the 20 days of the request being received, there is no requirement to release the information, but a delay in destruction may be considered. In these circumstances please refer to the trust's Freedom of Information Lead for further guidance.

Schedule for Retention

The NHS Code of Practice in Records Management has a schedule showing the minimum retention periods for records held by the Trust (Appendix 12 for link to schedule). The schedule determines whether records are to be selected for permanent preservation, destroyed or retained by the Trust for research or litigation purposes. Whenever the schedule is used, the guidelines listed below should be followed:

- Local business requirements/instructions must be considered before activating retention periods in this schedule.
- Decisions should also be considered in the light of the need to preserve records whose use cannot be anticipated fully at the present time, but which may be of value to future generations.
- Recommended minimum retention periods should be calculated from the end of the calendar or accounting year following the last entry on the document.
- Where it is indicated that the documents described must be considered for permanent preservation and the advice of the chief archivist of an appropriate place of deposit obtained.
- The provisions of the Data Protection Act 1998 must also be complied with.

App 9
Disposal Form

Worcestershire NHS
Acute Hospitals NHS Trust

DISPOSAL FORM FOR RECORDS DOCUMENTS

Record Reference	Record Type/Description	Disposal Date

The above records have been disposed of in accordance with the Records Management Policy of the Trust.

Signed:……..Date:……
Departmental Manager

Signed:……..Date:……
Senior Manager

App 10
Archiving Form

Worcestershire NHS
Acute Hospitals NHS Trust

ARCHIVING OF RECORDS DOCUMENTS

Record Type	Date of Record	Ownership/ Disposal responsibility	Storage location (electronic/filing)	Box No	Aisle No	Retention Period	Disposal Date	Lead	Comments

The above records have been archived of in accordance with the Records Management Policy of the Trust.

Signed:……..Date:……

Departmental Manager

Signed:……..Date:……

Senior Manager

How to deal with specific types of records

We have written this section to deal with a number of issues raised by health and social care records managers to TNA, the NHS Digital and the DH between 2009 and the end of 2015 since the previous Code was issued in 2006.

These issues relate to the following health and social care records:

- Records at Contract Change
- Integrated Records
- Integrated Viewing Technology and Record Keeping
- Complaints Records
- Specimens and Samples
- Continuing Care Decisions Records
- Records of Funding
- Health Records of Transgender Persons
- Witness Protection Health Records
- Controlled Drugs Regime
- Occupational Health Records
- Records of non-NHS funded patients treated on NHS premises
- Patient/Client Held Records
- Staff Records
- Email and Record Keeping Implications
- Records Created via Social Media
- Records Created Through Bring Your Own Device (BYOD)
- Cloud Based Records
- Website as a Business Record
- Scanned Records
- Duplicate Records
- Edisclosure/Ediscovery and Records Implications

Records at Contract Change

Once a contract ends, any service provider still has a liability for the work they have done and as a general rule at any change of contract the records must be retained until the time period for liability has expired.
In the standard NHS contract there is an option to allow the commissioner to direct a transfer of care records to a new provider for continuity of service and this includes third parties and those working under any qualified provider contracts. This will usually be to ensure the continuity of service provision upon termination of the contract. It is also the case that after the contract period has ended; the previous provider will remain liable for their work. In this instance there may be a need to make the records available for continuity of care or for professional conduct cases.

Where legislation creates or disbands public sector organisations, the legislation will normally specify which organisation holds liability for any action conducted by a former organisation. This may also be a consideration to identify the legal entity which must manage the records. Where the content of records is confidential, for example care records, it may be necessary to inform the individuals concerned about the change. Where there is little impact upon those receiving care it may be sufficient to use posters and leaflets to inform people about the change, but more significant changes may require individual communications or obtaining explicit consent. Although the conditions of the DPA may be satisfied in many cases there is still a duty of confidence which requires a patient or client (in some cases) to agree to the transfer.

It is vital to highlight the importance of actively managing records which are stored in offsite storage. This will ensure that the organisation maintains a full inventory of what is held offsite, retention periods are applied to each record, a disposal log is kept, and privacy impact assessments are conducted on the offsite storage providers. Table 6 summarises some possible scenarios and, for each option, patient consent and information sharing agreement or a contract may be required to share the information. See the Records Management Code of Practice for Health and Social Care 2016 for further guidance.

Integrated Records

Integrated or joint care records create additional issues which must be resolved locally. This includes a means of attributing ownership and access to the records between all parties where there is a lawful basis to access the records.

These arrangements may include:

- Nominating one organisation to own the records
- Separating the records so that each party retains their own information
- Each party keeps their own record but has access to the shared part of the other record.

For each option, some form of patient consent is necessary to enable all parties to access information lawfully. An information sharing agreement is recommended as a mechanism for providing clarity and transparency on the standards that all participants must meet.

Integrated Viewing Technology and Record Keeping

Many record keeping systems pool records to create a view or portal of information which can then be used to inform decisions. This in effect creates a single digital instance of a record which is only correct at the time of viewing. Where these are used, it may be necessary to recreate the instance of viewing to allow an audit trail of decision making. It may be necessary to make a note in the record that the information has been obtained by this means to attribute the source of evidence for any interventions taken.

Complaints Records

Where a patient or client complains about a service, it is necessary to keep a separate file relating to the complaint and subsequent investigation. Complaint information should never be recorded in the clinical record. A complaint may be unfounded or involve third parties and the inclusion of that information in the clinical record will mean that the information will be preserved for the life of the record and could cause detrimental prejudice to the relationship between the patient and the health care team.

Where multiple teams are involved in the complaint handling, all the associated records must be amalgamated to form a single record. This will prevent the situation where one part of the organisation does not know what the other has done. It is common for the patient or client to ask to see a copy of their complaint file and it will be easier to deal with if all the relevant material is in one file. Where complaints are referred to the Ombudsman Service a single file will be easier to refer to. The ICO has issued guidance on complaints files and who can have access to them, which will drive what must be stored in them.

Specimens and Samples

The retention of human material is not covered in this Code and is not in scope. The metadata or information about the sample or specimen is in scope. Relevant professional bodies such as the Human Tissue Authority or the Royal College of Pathologists have issued guidance on how long to keep human material.

Just because the human material is not kept for long periods, does not mean that the information about the specimen or sample must be destroyed at the same time. The information about any process involving human material must be kept for continuity of care and legal obligations. The correct place to keep information about the patient is the clinical record and although pathology reports may be retained by the individual pathology departments, a copy must always be included on the patient record.

Continuing Care Decisions Records

In order to process applications and appeals for funding continuing care, it is necessary for the relevant organisation to have access to clinical records. This will be based on consent and organisations need to have arrangements in place to facilitate sharing or put systems in place to allow access to view records or take copies. Any access must be lawful and the decision to grant access recorded.

Records of Funding

Funding records are primarily administrative records but they contain large amounts of care information and as such must be managed as clinical records for their access and management. This includes having rigorous processes for access and the appropriate lawful basis to share them.

Health Records of Transgender Persons

A patient can request that their gender be changed in a record by a statutory declaration, but this does not give them the same rights as those that can be made by the Gender Recognition Act 2004. The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Certificate is issued by a Gender Reassignment Panel. At this time a new NHS number can be issued and a new record can be created, if it is the wish of the patient. It is important to discuss with the patient what records are moved into the new record and to discuss how to link any records held in any other institutions with the new record.

Witness Protection Health Records

Where a record is that of someone known to be under a witness protection scheme, the record must be subject to greater security and confidentiality. It may become apparent (such as via accidental disclosure) that the records are those of a person under the protection of the Courts for the purposes of identity. The right to anonymity extends to medical records. For people under certain types of witness protection, the patient will be given a new name and NHS Number, so the records may appear to be that of a different person.

Controlled Drugs Regime

NHS England in conjunction with the NHS Business Services Authority has established procedures for handling information relating to controlled drugs. This guidance includes conditions for storage, retention and destruction of information. Where information about controlled drugs is held please refer to NHS England guidance.

Occupational Health Records

Occupational health records are not part of the main staff record and for reasons of confidentiality they are held separately. However, it is permitted for reports or summaries to be held in the main staff record where these have been requested by the employer and agreed by the staff member. When occupational health records are outsourced, the organisation must ensure that any contractor can retain the records for the necessary period after the termination of service for purposes of adequately recording any work based health issues.

Records of non-NHS funded patients treated on NHS premises

Where records of individuals who are not NHS or social care funded are held in the record keeping systems of NHS or social care organisations, they must be kept for the same minimum retention periods as other records outlined in this Code. The same levels of security and confidentiality will also apply.

Patient/Client Held Records

Where it is necessary to leave records with the individual who is the subject of care, it must be indicated on the records that they remain the property of the issuing organisation and include a return address if they are lost. Organisations must be able to produce a record of their work which includes services delivered in the home where the individual holds the record. Upon the termination of treatment where the records are the sole evidence of the course of treatment or care, they must be recovered and given back to the issuing organisation. An example of this would be the maternity file that is held by the mother until the first GP visit after the birth of the baby or until it is no longer required.

A copy can be provided if the individual wishes to retain a copy of the records. Where the individual retains the actual record after care, the organisation must be satisfied it has a record of the contents. An example is a child's red book where the parent retains the record but the contents are also recorded in the health visiting file.

Staff Records

Staff records should hold sufficient information about a staff member for decisions to be made about employment matters. The nucleus of any staff file will be the paperwork collected through the recruitment process and this will include the job advert, application form, right to work, identity checks and any correspondence relating to acceptance of the contract. The central file must be the repository for this information.

It is common practice for the line manager to hold staff records which can contain large portions of an employee's employment history (for example training records). This practice runs the risk of much of the employment record being lost if there is an internal move of the employee or upon termination of contact. It is important that there is a single record of the employment of an employee.

Upon termination of contract, records must be held up to and beyond their statutory retirement age. Staff records may be retained beyond 20 years if they continue to be required for NHS business purposes, in accordance with Retention Instrument 122. They are not exempt from Principle 5 of the DPA.

To reduce the burden of storage and for reasons of confidentiality it is recommended that a summary be prepared and held until the employee's 75th birthday or 6 years after leaving whichever is the longer and then reviewed.

Where a summary is made it must contain as a minimum:

- A summary of the employment history with dates
- Pension information including eligibility
- Any work related injury
- Any exposure to asbestos, radiation and other chemicals which may cause illness in later life
- Professional training history and professional qualifications related to the delivery of care
- List of buildings where the member of staff worked and the dates worked in each location.

Disciplinary case files can be held in a separate file so they can be expired at the appropriate time and do not clutter up the main file. That does not mean that there should be no record that the disciplinary process has been engaged in the main record.

Email and Record Keeping Implications

One of the most important, yet often neglected, containers of information are the email accounts of staff, which is why it deserves a special mention in this Code. Email has the benefit of fixing information in time and assigning the action to an individual, which are two of the most important characteristics of an authentic record.

A common problem with email is that it is rarely saved in the business context, which is the third characteristic to achieve an authentic record. The correct place to store email is in the record keeping system according to the business classification scheme or file plan activity to which it relates. Solutions such as email archiving and ever larger mailbox quotas do not encourage staff to meet the standard of storing email in the correct business context and to declare the email as a record.

Where email archiving solutions are of benefit is as a backup, or to identify key individuals where their entire email correspondence can be preserved as a public record. Where email is declared as a record or as a component of a record, the entire email must be kept including attachments so the record remains integral - for example an email approving a business case must be saved with the business case file.

All staff need to be adequately trained in required email storage and organisations need to undertake periodic audits of working practice to identify and address poor practice.

Automatic deletion of email as a business rule may constitute an offence under Section 77 of the FOIA where it is subject to a request for information even if the destruction is by automatic rule. The Courts' civil procedure rules 31(B) also require that a legal hold is placed on any information including email when an organisation enters into litigation.

Legal holds can take many forms and records cannot be destroyed if there is a known process or an expectation that records will be needed for a future legal process. This may include national or local inquiries, criminal investigation, and expected cases of litigation or records that may be requested under FOI or subject access.

This means that no records can be destroyed by a purely automated process without some form of review whether at aggregated or individual level for continued retention or transfer to a place of deposit.
The NHS mail system allows a single email account for every staff member that can follow the individual through the course of their career. When staff transfer from one NHS organisation another NHS organisation, they must ensure that no sensitive personal data relating to the former organisation is transferred.

It is good practice for staff to purge their email accounts of information upon transfer to prevent a breach of confidence or the transfer of security classified information. This is facilitated by staff storing only those that need to be retained on an on-going basis. Emails that are the sole record of an event or issue, for example an exchange between a clinician and a patient, should be copied in to the relevant clinical record rather than being simply deleted.
Email archive

Whilst Email is not intended to be a filing system, the archiving facilities can provide a means of meeting the retention periods as detailed in the retention and disposal schedule of the Records Management Policy. Emails should be kept if they constitute a business record, note that if the information is in a document attached to the e-mail then the attachment should be saved within the normal document management system of the department (e.g. folder in the M:\ drive). Emails which need to be retained can also be stored in this way.
NHS mail has its own retention policy – http://systems.hscic.gov.uk/nhsmail/policies/retention.pdf
The Trust has a mail archiving solution called Mail safe. This solution stores any email that was present in the Exchange email system (pre March 2016). Staff who had a @worcsacute.nhs.uk email address will have email stored in the archiving solution. Staff who joined the Trust and only received a @nhs.net email address will not have email archived into the Mail safe solution.

Records Created via Social Media

Where social media is used as a means of communicating information for business purposes or it is a means of interacting with clients, it may be a record that needs to be kept. Where this is the case, information must be retained within the record keeping system. This may not necessarily mean that the social media must be captured but rather the information of the activity through transcription or periodic storage.

Records Created Through Bring Your Own Device (BYOD)

Any record that is created in the context of health and social care business is the intellectual property of the employing organisation and this extends to information created on personally owned computers and equipment. This in turn extends to emails and text messages sent in the course of business on personally owned devices from personal accounts. They must be captured in the record keeping system if they are considered to fall within the definition of a record.

When an individual staff member no longer works for the employing organisation, any information that staff take away could be a risk to the organisation. If this includes sensitive personal data, this is reportable to the ICO and may be a breach of confidentiality. For this reason it is not permitted to store patient confidential data on any insecure device or system that does not meet national requirements. The IGA has issued a guide for BYOD which clarifies the issues.

Cloud Based Records

Use of cloud based solutions for health and social care are increasingly being considered as an alternative to managing large networks and infrastructure. Before any cloud based solution is implemented there are a

number of records considerations that must be addressed. The ICO has guidance on cloud storage they also advise to conduct a privacy impact assessment for any potential cloud solutions.

The NHS has a prohibition on storing patient identifiable data outside of England where there is any link to national systems or applications (e.g. N3 or NHS mail), so any solution must have servers that can be traced to England if it is going to be used to store patient data.

Another important consideration is that at some point the service provider or solution will change and it will be necessary to migrate all of the records, including all the formats, onto another solution and this may be technically challenging.

Records in cloud storage must be managed just as records must be in any other environment and the temptation to use ever increasing storage instead of good records management will not meet the records management recommendations of this Code.
Where personal data is stored there is also the risk of breaching the requirements of the DPA not to store personal information longer than necessary.

Website as a Business Record

As people interact with their public services, more commonly it is the internet and websites in particular that provide information, just as posters, publications and leaflets once did exclusively.
A person's behaviour may be a result of interaction with a website and it is considered part of the record of the activity.

For this reason, websites form part of the record keeping system and must be preserved. It is also important to know what material was present on the website as this material is considered to have been published. Therefore, the frequency of capture must be adequate, or some other method to recreate what the website or intranet visitor viewed.

It may be possible to arrange regular crawls of the site with the relevant place of deposit, but given the complexity of sites as digital objects, it may be necessary to use other methods of capture to ensure that this creates a formal record.

The UK Government Web Archive (part of TNA) undertook two central crawls of all NHS sites in 2011 and 2012 and may have captured some from 2004 onwards, but the information captured will not include all levels of the sites or some dynamic content.

Scanned Records

This section applies to health and care records as much as it does to corporate records.
Where scanning is used, the main consideration is that the information can perform the same function as the paper counterpart did and like any evidence, scanned records can be challenged in a court. This is unlikely to be a problem provided it can be demonstrated that the scan is an authentic record and there are technical and organisational means to ensure the scanned records maintain their integrity, authenticity and usability as records, for the duration of the relevant retention period.

If this is a record type which must or may be selected and transferred to a place of deposit, the place of deposit should be asked whether they wish to preserve the hard copy and/or the scans. If the hard copy is retained, this will constitute 'best available evidence' for legal purposes, rather than the scanned copy.
The legal admissibility of scanned records, as with any digital information, is determined by how it can be shown that it is an authentic record. An indication of how the courts will interpret evidence can be found in the civil procedure rules and the court will decide if a record, either paper of electronic, can be admissible as evidence.

The standard, 'BS 10008 Electronic Information Management - Ensuring the authenticity and integrity of electronic information', specifies the method of ensuring that electronic information remains authentic. The standard deals with both 'born digital' and scanned records. The best way to ensure that records are

scanned to the appropriate standard is to use a supplier or service that meets the standard. It is expected that all large scale digitisation projects will receive assistance from industry experts to ensure that the records are scanned to standard.

For small scale scanning requirements or those records where there is a low risk of being required to prove their authenticity, organisations may decide to do their own scanning.
Once scanned records have been digitised and the appropriate quality checks completed, it will then be possible to destroy the paper original. A scan of not less than 300 dots per inch (or 118 dots per centimetre) as a minimum is recommended for most records although this may drop if clear printed text is being scanned.

Methods used to ensure that scanned records can be considered authentic are:

- A written procedure outlining the process to scan, quality check and any destruction process for the paper record
- Evidence that the process has been followed
- An audit trail or secure system that can show that no alterations have been made to the record after the point they have been digitised
- Fix the scan into a file format that cannot be edited such as Portable Document Format (PDF).

Before you begin scanning, check that those for whom you may have to produce records for will accept an authentic copy.

Some common mistakes occur in scanning by:

- Only scanning one side and not both sides, including blank pages
- Scanning a copy of a copy leading to a degraded image
- Not using a method that can show that the scanned record has not been altered after it has been scanned
- Not having a long term plan to enable the digitised records to be stored or accessed over the period of their retention.

Duplicate Records

Within any record keeping system, there is a primary instance which can be considered the version that needs to be kept and this will be normally be held by the person or the team with the function to provide the service or activity about which the records relates.
It is not necessary to keep duplicate instances of the same record unless it is used in another process and is then a part of a new record. An example of this is incident forms. Once the information is transcribed into the incident management system, there is no longer a need to hold the (now) duplicate instance of the original form used to record the incident. Where clinical systems produce duplicate records such as print outs of clinical records these must be marked as a copy to prevent their use as a primary record.

Edisclosure/Ediscovery and Records Implications

In UK Law, the civil procedure rules allow evidence to be prepared for court and, as part of this; the parties in litigation can agree what documents they disclose to the other party and dispute authenticity. In some jurisdictions this is called discovery, but in UK the process is known as disclosure. The disclosure of electronic records is referred to as Edisclosure or Ediscovery.
The relevant rule for disclosure and admissibility of evidence is given in the Ministry of Justices Civil Procedure Rules' Rules and Practice Directions as Rule 31. Proof statements can be required in some cases.
If records are arranged in an organised filing system, such as a business classification scheme, or all the relevant information is placed on the patient or client file, this process will be much easier to provide documents as evidence.

NATIONAL RETENTION AND DISPOSAL SCHEDULE

Please refer to the Retention and Disposal Schedule (Available on document finder)

For a full list of retention periods

Appendix 13	Worcestershire NHS Acute Hospitals NHS Trust

Records Inventory Collection Form

Worcestershire NHS
Acute Hospitals NHS Trust

Date Form Completed:	
Department/Service:	
Site/Location:	
Directorate:	
Contact Name:	
Job Title:	
Telephone Number:	
The form is designed to record information for both Manual and Electronic records. Please complete all sections labelled ALL, and any sections that relate to your records - Manual (M) or Electronic (E) The sections coloured in BLUE are drop down lists to select from	
Do you store manual or electronic records in the department	**Please click on drop down list and select answer:**
ALL RECORDS: What is the name of the Record or the system where the records are held?	
ALL RECORDS: List the alternative name of the record if appropriate	

ALL RECORDS: Please describe the record: type, use etc.		
ALL RECORDS: Are duplicates of the record held?	**Please click on drop down list and select answer:**	**Why and Where:**
ALL RECORDS: Who is responsible for managing the record (if different from name at top of form)?	**Please include Name, Job Title and contact number:**	
ALL RECORDS: What is the format of the record?	**Please click on drop down list and select answer:**	**Other - Please Specify:**
ALL RECORDS: Do you consider retention of the record at the point of creation? This may be marking records at creation to allow archiving/destruction easier in the future.	**Please click on drop down list and select answer:**	**Please Specify:**
ALL RECORDS: Why do you create/collect this information?	**Please click on drop down list and select answer:**	**Other - Please Specify:**
ALL RECORDS: Where does this information originate from?	**Please click on drop down list and select answer:**	

ALL RECORDS: Does the record contain personal data?	**Please click on drop down list and select answer:**	**Please Specify:**
ALL RECORDS: Is access to the record, or information it contains, restricted to within the department or is it shared WITHIN THE TRUST?	**Please Select: Shared with whom?**	**Comments:**
	Please Select: Why is it shared?	**Comments:**
	Please Select: Does it include access to personal data?	**Comments:**
ALL RECORDS: Is the record, or information it contains, shared with others from OUTSIDE THE TRUST?	**Please Select: Shared with whom?**	**Comments:**
	Please Select: Why is it shared?	**Comments:**
	Please Select: Does it include access to personal data?	**Comments:**
MANUAL RECORDS: How many records are held? (estimate)	**Total records:**	**Approx.:**
	Active Records (if known):	**Approx.:**
	Inactive Records (if known):	**Approx.:**
ALL RECORDS: Is there a register or index etc. of the records?	**Please click on drop down list and select answer:**	**Please Specify:**
ELECTRONIC RECORDS: Are paper records scanned to make the electronic record?	**Please click on drop down list and select answer:**	**Please Specify:**

ELECTRONIC RECORDS: Where are the electronic records stored?	**Please click on drop down list and select answer:**	**Please Specify:**
MANUAL RECORDS: Where are the MANUAL records stored? (e.g. Nurses office – Ward - Department - Area	**Please Specify:**	
MANUAL RECORDS: Is there currently sufficient storage available?	**Please click on drop down list and select answer:**	**Please Specify:**
MANUAL RECORDS: Will sufficient storage be available in the future?	**Please click on drop down list and select answer:**	**Please Specify:**
MANUAL RECORDS: Are these locations secured? (e.g. locked cabinets, rooms etc.)	**Please click on drop down list and select answer:**	**Comments:**
MANUAL RECORDS: Do you have procedures in place to ensure secure notes are available when needed? (able to access locked areas etc.)	**Please Click on drop down list and select answer:**	**Comments:**
MANUAL RECORDS: Are any of the storage areas: If answer is yes, please add details	**Shared with the cleaner, other depts. etc.**	
	Outside building (e.g. garage, porta cabin etc.)	
	Structurally unsound	
	Evidence of damp, dry rot, pests etc.	
	Inadequate lighting	

	Inappropriate/insufficient shelving	
	Dirty/messy	
	Unsafe to work in	
MANUAL RECORDS: Do you have manual records stored off site?	**Please Specify:**	
ELECTRONIC RECORDS: What is the backup system in case of system failure?	**Please Specify:**	
ALL RECORDS: Do you have a record tracking system should records leave the department?	**Please click on drop down list and select answer:**	**Comments:**
ALL RECORDS: How are records transferred, should they leave the dept.	**Please Specify:**	
ALL RECORDS: Is there a business continuity plan for the records? (disaster recovery etc.)	**Please click on drop down list and select answer:**	**Please Specify:**
Retention		
ALL RECORDS: Have you identified how long the records must be kept	**Please click on drop down list and select answer:**	**Please Specify:**

ALL RECORDS: Do you have a plan for dealing with records that are due for appraisal? (Volume etc.)	**Please click on drop down list and select answer:**	**Please Specify:**
ALL RECORDS: Do you have an established procedure for closing records when they are no longer current?	**Please click on drop down list and select answer:**	**Please Specify:**
ALL RECORDS: Do you have any records that should be assessed for permanent preservation?	**Please click on drop down list and select answer:**	**Please Specify:**
ALL RECORDS: What action is taken when the retention period is exceeded?	**Please click on drop down list and select answer:**	**Please Specify:**
MANUAL RECORDS: When paper records are no longer live but are not at the correct retention period, where are they stored and are the correct provisions for access and retrieval in place and standards are met to ensure no environmental damage is caused?	**Please Specify:**	
ALL RECORDS: Have you identified a secure and confidential method for the disposal of records, and have processes to organise the disposal?	**Please click on drop down list and select answer:**	**Please Specify:**

ALL RECORDS: Do you maintain a log of records which have been destroyed showing their reference, description and date of destruction?	**Please click on drop down list and select answer:**	**Please Specify:**
Further Comments: if you have any further comments or questions regarding the information that you hold (e.g. Creation, Maintenance, Storage, Retention, Disposal etc.) please specify below:		

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