Worcestershire Health and Care NHS
NHS Trust

RECORDS MANAGEMENT POLICY

Document Type	Corporate Policy
Unique Identifier	IG-006
Document Purpose	This policy provides assurance that corporate and patient records are dealt with legally, securely, efficiently and effectively, in order to deliver the best possible high quality patient care
Document Author	Maureen Bottrell, Records Manager
Target Audience	All Worcestershire Health and Care NHS Trust staff
Responsible Group	Worcestershire Health and Care NHS Trust, Information Governance Steering Group / Records Management Steering Group
Date Approved	17 November 2016
Expiry Date	December 2019
Equality Impact Assessment	This Policy has been screened using the Equality Duty Assessment Form and does not require a full Equality Impact Assessment

This validity of this procedure is only assured when viewed via the Worcestershire Health and Care NHS Trust website (hacw.nhs.uk). If this document is printed into hard copy or saved to another location, its validity must be checked against the unique identifier number on the internet version. The internet version is the definitive version.

If you would like this document in other languages or formats (i.e. large print), please contact the Communications Team on 01905 760020 or email WHCNHS.Communications@nhs.net

Version History

Version	Circulation Date	Job Title of Person/Name of Group circulated to	Brief Summary of Change
0.1	21/11/2011	Records Management Group	Update to contact list
0.2	16/03/2012	IG Steering Group	Approved
1.0	28/03/2012	Quality and Safety Committee	Ratified
1.1	06/11/2013	Mental Health Act / Patient Records Manager Head of Information Governance	Update document removing references to NHS Worcestershire
2.0	08/11/2013	Mental Health Act / Patient Records Manager	Updated guidance on creation of case notes
2.2	10/11/2016	Records Management Group, Head of Information Governance	Updated retention periods guidance
3.0		Quality and Safety Committee	Ratified
3.1	14/9/2018	Head of Quality Governance	Amendment – no longer requirement for countersigning clinical notes.
3.2	22/10/2018	Data Protection Officer	Updated for GDPR legislative changes

Accessibility

Interpreting and Translation Services are provided for Worcestershire Health and Care NHS Trust, including:

- Face to face interpreting;
- Instant telephone interpreting;
- Document translation, and
- British Sign Language interpreting.

Please refer to intranet page: http://nww.hacw.nhs.uk/a-z/services/interpreting-and-translation-services/ for full details of the service, how to book and associated costs.

Co-production

Co-production reflects the values of the NHS Constitution which promotes the full involvement of patients, staff, families, carers and professionals inside and outside the NHS. The Trust expects that all healthcare professionals will provide clinical care in line with best practice. In offering and

delivering that care, healthcare professionals are expected to respect the individual needs, views and wishes of the patients they care for, and recognise and work with the essential knowledge that patients bring. Staff will demonstrate a respect for patient diversity and a capacity to respond with flexibility. As facilitators of care, staff will work with patients and carers to help them understand their diagnosis and treatment options. Staff bring knowledge and expertise to enable and empower patient partners to make the right choices for themselves.

Training and Development

Worcestershire Health and Care NHS Trust recognise the importance of ensuring that its workforce has every opportunity to access relevant training. The Trust is committed to the provision of training and development opportunities that are in support of service needs and meet responsibilities for the provision of mandatory and statutory training.

All staff employed by the Trust are required to attend the mandatory and statutory training that is relevant to their role and to ensure they meet their own continuous professional development.

Contents **Page No**

1. Introduction

a. Worcestershire Health and Care NHS Trust (the Trust) is dependent on its records to operate efficiently and to account for its actions. This policy defines a structure for the organisation to ensure adequate records are maintained, managed and controlled effectively and at best value, commensurate with legal, operational and information needs. This policy is an overarching policy designed to provide all professionals working within the Trust with information on the principles of good documentation and record keeping within their administrative and clinical practice and to ensure consistent standards across professional groups. In addition, to complement this policy there is specific guidance for the management of clinical records, for archiving paper records and guidance for staff on access to health records.

b. 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, efficiency and productivity and help us deliver our services in consistent and equitable ways.

2. Purpose

a. An effective records management policy ensures that such information is properly managed and available to support:

   i. Patient care

   ii. The day-to-day business, which underpins care delivery

   iii. Evidence-based practice/care pathways

   iv. Management decision-making

   v. Partnership working

   vi. Legal requirements including General Data Protection Regulation/ Data Protection Act and Freedom of Information Act

   vii. Medical, organisational and miscellaneous audits

   viii. Improvements in clinical effectiveness through research

   ix. Clinical Governance

   x. Research Governance

   xi. Reduction in aspects of risk

   xii. 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.

   xiii.

3. Scope

a. This policy relates to **all** operational records.

b. Operational records are defined as information, created or received in the course of business, and captured in a readable form in any medium, providing evidence of the functions, activities and transactions. They include:

i. Administrative records (including personnel, estates, financial and accounting records, contract records, litigation and records associated with complaint-handling)

ii. Patient health records, including those concerning all specialities but excluding GP medical records

iii. Theatre Registers and all other registers that may be kept

iv. X-Ray and imaging reports, output and images

v. Photographs, slides, and other images

vi. Microform (i.e. fiche/film)

vii. Audio and video tapes, cassettes

viii. Records in all electronic formats e.g. email

c. They do not include copies of documents created by other organisations such as the Department of Health, kept for reference and information only.

d. All records created in the course of the business of the Trust are corporate records and are public records under the terms of the Public Records Acts 1958 and 1967. This **includes** email messages and other electronic records. Further guidance in relation to electronic records is provided in section 15.

e. The Trust must ensure that it adheres to all legislation and guidance in relation to Records Management. The Trust should:

i. Ensure there are strict guidelines in the formation of records and information, whether it is manual or computerised.

ii. Maintain, archive and track these records to ensure their use and validity.

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

iv. Store and preserve records in an environment where they are not susceptible to damage or destruction.

v. 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.

vi. Comply with and ensure all Trust employees know the importance of security and confidentiality of information and records by offering training in all departments and services.

vii. Understand and comply with legislation and keep up to date on current issues relating to records management.

f. 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 line with this document. This policy 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

g. In addition to this policy, all clinical staff working for the Trust should adhere to other Trust record keeping guidance, and in particular the Trust Clinical Record Keeping Guidelines and the guidelines laid down by appropriate professional regulatory bodies.

h. This policy is mandatory for all staff working within the Trust.

4. Legal and professional obligations

a. All NHS records are Public Records under the Public Records Acts and must be kept in accordance with statutory and NHS guidelines, in particular:

   i. Public Records Acts 1958 and 1967

   ii. European Union General Data Protection Regulation / Data Protection Act 1998 (GDPR/DPA18)

   iii. Freedom of Information Act 2000

   iv. Records Management Code of Practice for Health and Social Care 2016

   v. Clinical Negligence Scheme for Trusts (CNST)

   vi. The Caldicott Principles

   vii. Care Quality Commission

   viii. Audit Commission, Setting the Record Straight, 1995

   ix. Information Security Policy

   x. Common Law Duty of Confidentiality

   xi. Confidentiality: NHS Code of Practice

   xii. Independent Inquiry into Child Sexual Abuse (IICSA) 2016

b. 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. The appropriate documentation within Worcestershire is the Worcestershire Standard for Sharing Personal Data and guidance on its implementation and formulation of protocols can be found on the Trust Intranet.

5. Policy objectives

The main objectives of this policy are:

a) Accountability – That adequate records are maintained to account fully and transparently for all actions and decisions in particular:

   i. To protect legal and other rights of staff or those affected by those actions

   ii. To facilitate audit or examination

   iii. To provide credible and authoritative evidence

b) Quality – that records are complete and accurate and the information they contain is reliable and its authenticity can be guaranteed.

c) Accessibility – that records and those with a legitimate right of access can efficiently retrieve the information within them, for as long as the records are held by the Trust

d) 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.

e) Retention and disposal – that there are consistent and documented retention and disposal procedures to include provision for permanent preservation of archival records.

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

In addition, this policy aims to provide guidance on:

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

ii. **Records are available when needed** - from which the Trust is able to form a reconstruction of activities or events that have taken place

iii. **Records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist

iv. **Records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records

v. **Records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated

vi. **Records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format

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

viii. **Records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value

ix. **Staff are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management

6. Responsibilities and duties

a. **Trust Board**

i. Setting policy for the organisation through powers delegated to relevant committees

ii. Ensuring policy is implemented through agreed management arrangements

iii. Ensuring they are alerted to relevant issues arising that may affect policy

b. **Chief Executive**

i. ensuring that arrangements are in place so that employees are fully aware of their statutory, organisational and professional responsibilities and that they are fulfilled

ii. ensuring that the arrangements in support of policy are fully implemented through inclusion in Service Delivery Unit Performance Reviews

iii. in order for this responsibility to be effectively discharged, Executive Directors and senior colleagues will have specific delegated responsibility to support the Chief Executive in this process

iv. the quality of records management across the Trust

c. **Caldicott Guardian**

i. lead for records management

d. **Directors** must ensure:

i. strategic development and implementation of policy, corporately and within their areas of control

ii. the appropriate assessment and management of risks

iii. effective delegation of responsibilities within their areas of control

iv. effective support for managers' decisions and recommendations in terms of the provision of appropriate resources

v. a framework is in place to ensure that staff are adequately skilled and experienced to safely undertake their work

vi. necessary reporting procedures are in place

vii. a framework is in place to monitor compliance with policy

e. **All Managers (Service Delivery Unit leads, Senior Managers, Ward and Team managers**

i. managers in all departments need to ensure that staff are aware of the current rules on such issues as Data Protection and access to patient information

ii. managers should ensure that staff are suitably trained in record keeping, security and storage of information/records (manual and computerised)

iii. managers should ensure an annual audit of a sample of records is undertaken and action plans as a result of the audits are implemented.

iv. line managers and supervisors must ensure that all staff are trained in the relevant aspect of record keeping dictated by their job role.

v. they should have mechanisms in place to ensure staff are trained in new legislation, procedures and policies as they arise. This should be in the form of induction training internally by the line manager of the department.

f. **Responsibility of all Employees**

i. 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.

ii. They must ensure that the records are kept up-to date and in good condition to have any real value to the Trust.

iii. 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 GDPR/DPA 2018.

iv. 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.

v. Patient/personal information must be processed in accordance with the requirements of the GDPR/DPA18 and the common law duty of confidentiality. Further details are included in the Trust's Code of Confidentiality for Employees

vi. 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.

vii. 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.

g. **Personal / Professional Integrity**

i. 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.

ii. 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.

iii. Professionals are accountable for the consequences of entries made by unqualified members of staff.

iv. Only registered clinical staff or non-registered staff who are assessed as competent should make clinical entries into the healthcare record.

v. Where the principle of a counter-signature can be applied then this practice should be adopted. A counter-signature is not however necessary. The accountability for record keeping standards remains with the registered practitioner, whether they have counter-signed the record or not.

vi. Clinical staff should refer to the Clinical Record Keeping Guidelines for detailed guidance.

h. **Responsibilities of Third Parties**

i. Anybody undertaking work for or with the Trust such as bank or agency staff, volunteers, locums, student placements and maintenance craftsmen must have contracts that detail the obligations on confidentiality and restrictions on the use of personal information, including those specified by the Records Management Code of Practice for Health and Social Care 2016, the Confidentiality: NHS Code of Practice and the GDPR/DPA18. The contract must require that patient information is treated and stored accordingly, and is used only for purposes consistent with the terms of the contract. Action that will be taken in the event of confidence being breached (e.g. termination of contract) should be specified within the contract.

7. Setting the NHS standard

a. A systematic and planned approach to the management of records within the Trust, from the moment they are created to their ultimate disposal, ensures that the Trust can:

   i. Control both the quality and the quantity of the information that it generates

   ii. Maintain the information in a manner that effectively services its needs, those of government and of the citizen

   iii. Dispose of the information efficiently when it is no longer required. This applies to all records whether manual or computerised records.

b. Records are valuable because of the information they contain and that information is only usable if:

   i. It is correctly and legibly recorded in the first place

   ii. It, is then kept up to date

   iii. It is easily accessible when needed.

c. Good record keeping ensures that:

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

   ii. 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.

   iii. New staff can see what has been done, or not done, and why.

   iv. Any decisions made can be justified or reconsidered at a later date.

d. Good Records Management is essential for:

   i. Providing high quality patient care

   ii. Continuity of care

   iii. Effective communication and dissemination of information between members of multi-disciplinary health care teams

   iv. An accurate account of continuous assessment, treatment, and evaluation reflected in a care plan

   v. The ability to detect problems, such as changes in the patient's or client's condition, at an early stage

   vi. Corporate memory

   vii. Clinical liability

   viii. Historical purposes

   ix. Purchasing and contract service agreement management

   x. Financial accountability

   xi. Disputes or legal action

e. It is therefore important to ensure:

   i. Important and relevant information is recorded and completed

   ii. Handwritten records are legible, written in black ink, and can be easily read and reproduced when required

iii. Information/records are easily accessible and kept up-to-date

iv. Personal and patient identifiable information is shared rather than copied in order to reduce risks to confidentiality

v. Records are disposed of as soon as possible subject to national and local retention periods (Records Management Code of Practice for Health and Social Care 2016) or locally determined retention periods

vi. Records are shredded or disposed of in line with Trust procedure

f. What needs to be done to achieve best standards?

i. All Managers need to ensure that staff are aware of their personal responsibilities under the GDPR/DPA and familiar with Trust procedures for access to patient information.

ii. Managers should ensure that staff are suitably trained in record keeping, security and storage of information/records (manual and computerised).

g. Records may be required as evidence:

i. Before a court of law

ii. The Health Service Ombudsman

iii. The Information Commissioner

iv. In order to investigate a complaint at a local level

v. By Professional Conduct Committees e.g. NMC, which considers complaints about professional misconduct

8. Shared responsibility for NHS records

a. 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.

(1) **Statutory Responsibilities**

The Secretary of State for Health, Clinical Commissioning Groups, 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.

9. Creating records and record keeping standards

a. A record, whether it is in paper format or electronic, is a structured document which contains information, 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.

i. **New Referrals**

When new referrals are made to the Trust services, each team is responsible for checking whether the patient has an existing set of notes. Where the patient does not have an existing Case Note folder, do not immediately make up a folder; the following protocol should be observed:

1) Until a patient actually presents for their appointment, a case note folder should not be made up

2) Each team is responsible for keeping referral paperwork in a folder of some sort i.e. lever arch or ring binder

3) Referrals that are rejected or the patient DNAs (did not attend) should be kept in alphabetical order so that if the patient is re-referred, the paper work can be teamed up. A case note folder **should not** be made up at this stage.

4) DNA/Inappropriate referrals paperwork needs to be retained by the team for 2 years; it will not be filed within the Patient Records Departments.

5) After the 2 years has elapsed, paperwork can be destroyed by means of Printwaste confidential shredding services if the patient has not subsequently been re-referred to Trust Services.

ii. **Creating Case notes and Clinical Records**

Staff must ensure that clinical records are created in accordance with the Trust Clinical Record Keeping Guidelines.

(i) All records should have a unique file name or number and be part of a structured filing system. For example:

1. A patient's medical record will be identifiable by the patient's NHS Number.
2. An employee's personal file must be identifiable by the personnel number.

(ii) All records must have clear and precise formats.

a. They must be structured in the same way that files of the same description are structured with an easy to follow standardised index (either numerical, by date or alphabetically), so that information can be retrieved quickly and easily (for example all patient and employee files).

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

iii. **Updating Records**

(1) Managers should ensure that all records are regularly updated and maintained in a practical order.

(2) Staff should be vigilant when storing both electronic and paper files, to ensure their confidentiality, security and availability

(3) Records which are no longer required should be considered for archiving or disposal, depending on their statutory minimum retention period.

(4) 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.

(5) Concise and easy to follow procedures, whether they are paper or electronic systems, should back up all record keeping practices.

(6) Managers should ensure all staff are correctly trained.

ii. Please refer to the Trust Clinical Record Keeping Guidelines in relation to clinical record keeping

10. Using records and records tracking systems

a. 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.

b. A tracking system for all records should be in place to ensure that all information can be found quickly and easily.

c. 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 a spreadsheet 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.

d. Tracking systems should record the following (minimum) information:

   i. The reference number of the record (NHS /Personnel number and local identifier, box number where appropriate)

   ii. Any other applicable identifier i.e. department, hospital or ward code

   iii. Person, unit, department or place to where it is being sent

   iv. Date of transfer

   v. Date of information being received back (if applicable)

e. Managers should ensure that procedure notes and training are in place to maintain and regularly update the tracking system.

f. Managers should also ensure any tracking system is stored securely and access should only be given when applicable.

11. Records storage and retrieval

a. 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.

   i. Shelving and boxing

   (1) Records should be stored on shelves or in cabinets in a way which facilitates easy retrieval. This will not only provide for access to the records but will also make security checks more effective.

   (2) Paper records need not be boxed. Boxing may be required where, for example, there are risks from damage by excessive light, or where there is a high probability that certain records will be selected for permanent preservation.

   (3) 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.

(4) Computer disks and tapes should be stored in durable boxes not susceptible to mould, damp or water.

(5) Ideally computer, media and microfilm/fiche should be kept in a fireproof safe.

(6) Records should be stored off the floor to provide some protection from flood, dampness and dust.

(7) The width of aisles and general layout of storage areas must conform to fire, health and safety, and similar regulations.

(8) Large documents, such as maps, should be housed in special storage equipment to ensure that they are not damaged and are readily accessible.

(9) X-rays should be kept with patient's records at all times and extra care should be taken for exposure to light.

ii. Protection against fire and water

(1) All storage facilities should be protected by an automatic fire detection and alarm system including smoke detectors, installed and maintained.

(2) Portable fire extinguishers should be provided and should be installed at various points within the storage areas.

(3) Staff should be instructed in the location and use of fire fighting equipment, and fire drills should be undertaken.

(4) Records should not be stored where there may be a danger of flooding from pipes or radiators.

iii. Environment

(1) Unsuitable environments may cause irreversible damage to records more than any other factor.

(2) Managers must check humidity and ventilation within storage areas.

(3) Regular maintenance of heating and ventilation systems is essential.

(4) Managers must ensure fluctuations in temperature are monitored as they cause significant damage to the records, whether paper format or other media.

(5) If the humidity within the storage area rises at anytime, there is a great risk of mould growth. Managers must prevent this as damage could be irreversible to paper, microfilm/fiche or computer media.

iv. Transportation of records

(1) All records must be safeguarded from theft, damage or destruction. If a person's job role includes the transferring of records, the following guidelines must be adhered to.

a) By vehicle

i. Records should not be left unattended in the vehicle.

ii. They should not be left unattended at any location, unless in a locked facility.

iii. The person using the record at the time is responsible for their safekeeping.

iv. No one else in the vehicle should access the records unless they are authorised to.

b) By post

i. Records sent by post/porters should be carefully packaged to ensure they are not damaged en route. It is particularly important to ensure that records are packaged in a secure and robust fashion.

ii. They should be clearly labelled to the addressee, including Staff member Name. I.e. A. N. Other

iii. If they are to be delivered by the porters, then the porters should be given precise details of their destination, including Team Name, Office Name. I.e. Records Team, Company Secretary's Office, Isaac Maddox House

iv. No original records should be sent externally, instead produce a photocopy to be sent.

v. All copied records being sent externally must be sent by 'signed for delivery', to ensure a record of their journey is available in the event that they go missing.

vi. It must be noted on the record tracking system that the records have left their normal storage.

c) By electronic means:

a. Email

i. Records sent by email must be undertaken in line with the Countywide (Computacenter) Internet/Email Policy and the Trust Code of Conduct for Employees in respect of Confidentiality.

b. Fax

i. 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. For all faxes to a known Safe Haven please follow the guidance in the Trust Safe Haven Procedures.

ii. 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; Information is available on the Trust Intranet.

iii. Telephone the recipient to forewarn of the transmission and to confirm the number

iv. Use pre-programmed numbers wherever possible

v. Request that the recipient waits by the machine to receive the transmission

vi. Request that the recipient confirms receipt by telephone

vii. Ensure that there is a cover sheet that clearly states who the information is for and mark it "Private and Confidential"

viii. Check the recipient's number again before transmission

ix. Where possible, obtain a report print out from the machine to confirm successful transmission

d) Keeping patient records at home:

i. Please refer to the Trust protocol on 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. 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.

12. Confidentiality and accessing records

a. 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:

   i. Threat to personal safety or privacy

   ii. Embarrassment for the Trust and NHS

   iii. Legal obligation or penalty

   iv. Financial loss

   v. Disruption of activities

b. 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.

13. Selection of NHS records for permanent preservation

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

i. Permanent preservation at Local Authority Records Office

(1) The Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016, disposal and retention schedule highlights records likely to have an archival value.

(2) Departmental managers must identify which records they wish to preserve.

(3) Arrangements then should be made with the Local Authority Records Office for the transporting and storage of the records.

(4) A list should be made of all records sent for preservation.

(5) This includes records of paper, microfiche/ film and computer media.

(6) Access to the records will only be available through an arrangement with the Local Authority Records Office.

ii. Permanent preservation by electronic media

(1) Where a record is selected for permanent preservation by electronic media, then Computacenter should be contacted for further advice

(2) When the requirement is approved, the records will be fed through a scanner and the image of the record will appear on the screen.

(3) Once quality checks have been made, the record is then linked to an identifier.

(4) The record will either be stored on disk or on a computer network.

(5) The records can then be disposed of as per Section 15. A list of these records must be kept for future reference.

iii. Archiving and off-site storage of records

(1) When a record reaches the end of its statutory retention period, and there is no archival or research value, then the destruction of the record should be considered.

(2) Where a record is no longer in regular use or there is a lack of sufficient storage facilities, records can be sent for secure archiving on or off site.

(3) Once a decision has been made that a record is to be archived, then staff should follow the procedure described in the Trust's Off Site Archiving Procedure.

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

14. Disposal of records

a. The length of the retention period depends upon the type of record and its importance to the business of the Trust. The Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016 gives guidance on the retention and disposal of records (see summary in Appendix B). There may be additions to or deletions from the schedule to suit the needs of the Trust.

i. Process for disposal

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

c) It is the responsibility of the departmental manager or their deputy to identify the records, which can be destroyed.

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

e) Paper records should ideally be scanned into electronic format and then destroyed. This would apply to all medical and personnel records.

f) Records should be preserved forever in their original format.

g) Records should be destroyed completely.

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

i) Once the records have been scanned or the decision is made to destroy them then the manager should follow this procedure:

a) A list of all disposed records must be taken and kept indefinitely for audit purposes (Appendix C).

b) Contact your locality representative detailed in Appendix A for details of shredding arrangements in your locality.

c) If a contract for disposal needs to be arranged the Head of Procurement should ensure that the contract with the disposal company includes a confidentiality clause, which ensures adherence to the GDPR/DPA18 and common law.

d) The records should be placed in appropriate lockable storage bins for collection/on site shredding by the secure disposal company Print Waste.

e) For all archived records the department and senior manager must sign the destruction list (Appendix C) to confirm that the destruction of the records is approved, and the details of the actual disposal date must countersigned by the service lead for records management and retained for future reference by the Trust and Audit.

ii. Destruction of Records and the Freedom of Information Act 2000

(1) 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.

(2) If information has been deleted or destroyed under the Trust archiving guidelines, the applicant will need to be informed, with a justification for destruction.

(3) 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.

iii. Impact of the Independent Inquiry into Child Sexual Abuse (IICSA) and Destruction of Records

The Independent Inquiry into Child Sexual Abuse (IICSA), chaired by Professor Alexis Jay, has requested that large parts of the Health and Social Care sector do not destroy any records that are, or may fall into, the remit of the Inquiry. This includes children's records and any instances of allegations or investigations or any records of an institution where abuse has, or may have occurred. This may lead to specific future records management requirements.

Based upon the current scope of the IICSA Inquiry the Trust has approved records (appendix D) which could be destroyed in the expectancy that they pose minimal risk to these records containing information that will be of future relevance to the Inquiry. Those records which pose a high risk (appendix E) are recommended to be retained for the foreseeable future pending further clarification from IICSA Inquiry requirements.

iv. Schedule for Retention

(1) The Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016 has a suggested schedule showing the minimum retention periods for records held by the Trust (Appendix B is summary; the full Information Governance Alliance Records Management Code of Practice for Health and Social Care document is available on the Trust intranet). The schedule can determine 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:

a) Local business requirements/instructions must be considered before activating retention periods in this schedule.

b) 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.

c) Recommended minimum retention periods should be calculated from the end of the calendar or accounting year following the last entry on the document.

d) 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.

e) The provisions of the GDPR/DPA18 must also be complied with.

15. Confidentiality and security of records

a. 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 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.

b. The implementation of the GDPR/DPA18 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.

c. The guidelines contained within this policy underpin the principles of the GDPR/DPA18 and ensures that personal information is accurate, up to date and retrievable in a timely manner.

d. 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.

e. 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 Caldicott Guardian or the Data Protection Officer.

16. Electronic records

Including e-mail, memory sticks, dictation media – digital or tape:

a. Electronic information is subject to the same principles as paper records. In terms of minimum retention periods they are as shown in the Trust archiving guidelines

b. 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 this policy.

c. Staff who use memory sticks and/or dictation media, whether digital or analogue, for recording patient identifiable information such as notes of consultations or letters to other clinicians, shall be responsible for the security of these items whilst they are in their possession and use and until the media are handed directly to colleagues who are responsible for uploading and/or transcribing the information contained in the media.

17. Freedom of Information Act 2000

a. 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.

b. The Act gives a general right of access to all types of 'recorded information' held by public authorities, subject to certain conditions and exemptions.

c. Anyone 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'.

i. FOI Publication Scheme

(1) 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.

(2) The Trust FOI Publication Scheme is regularly updated and has been approved by the Information Commissioner.

(3) The Trust FOI Publication Scheme can be found on the website.

ii. Freedom of Information Act Policy

(1) The Trust FOI 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.

(2) The Policy will underpin any operational procedures and activities connected with the implementation of the Act.

(3) The FOI Policy applies to all Trust employees and non-executive directors.

(4) The Freedom of Information Act does not overturn the common law duties of confidence nor does it overturn the requirements of the GDPR/DPA18.

18. Audit, monitoring and training

a. Auditing records will help to ensure that the standard of the records are maintained and will serve to identify any areas for improvement and staff development. It is the responsibility of each departmental manager to ensure that records are audited annually and these are done in accordance with Trust procedures.

The audit will:

1) Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;

2) Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;

3) Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and

4) Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

5) The results of audits will be reported to the Trust Board.

b. Clinical Staff are required to audit their clinical records on an annual basis to meet the standards set by the NHSLA for the Risk Management Standard for Trusts. The documentation audit proforma included in the clinical records keeping policy should be used for this purpose.

c. Action plans must be developed where the audit reveals the standards of the Record Management Policy are not being met or maintained. Action plans must record who is responsible for leading against each action and the date by which action must be achieved.

d. All departmental managers are responsible for annual, localised monitoring of the quality of documentation and adherence to this policy. In particular, managers and senior clerical staff should undertake quality control checks to ensure that the standards, as detailed in this policy, are maintained.

e. All departmental managers are responsible for ensuring that staff attend mandatory training in clinical record keeping, case note handling and confidentiality.

19. Review of policy

a. This policy will be reviewed every three years.

b. Any new legislation and guidance from The Department of Health, The Information Governance Alliance and NHS Information Authority will be reflected in this policy and disseminated throughout the Trust. Appropriate training will be given where necessary.

20. Trust guidelines and procedures supporting this policy

a. Subject Access Request Standard Operating Procedure

b. Off Site Archiving Procedure

c. Clinical record keeping guidelines

d. Clinical record keeping audit template

Appendix A – Contacts for Archiving Records

RECORD LOCATION	CONTACT PERSON	CONTACT DETAILS
Adult Mental Health (Redditch and Bromsgrove)	Simon Hardy	simonhardy@nhs.net
Adult Mental Health Kidderminster and Wyre Forrest)	Gill Elcock	gillian.elcock@nhs.net
Adult Mental Health Worcester)	Nicola Jones	nichola.jones3@nhs.net
Business Development (includes Comms, Procurement and Programme Management Office)	Tracey Broadley	tbroadley@nhs.net
Child and Adolescent Mental Health Services (CAMHS) • Redditch and Bromsgrove • South Worcs • Wyre Forest	Phillipa Collins Lucy Hughes / Natasha Sheen Cormac Baddeley	phillipa.collins@nhs.net Lucy.Hughes5@nhs.net/Natasha.Sheen@nhs.net cormac.baddeley@nhs.net
Children's Services	Suzanne Claxton	suzanneclaxton@nhs.net
Community Care – Redditch and Bromsgrove	Beverley Banner	b.banner@nhs.net
Community Care – South Worcs	Kim Spooner	kim.spooner1@nhs.net
Community Care – Wyre Forest	Kate Butler	kate.butler5@nhs.net
Community Hospitals – Evesham / Pershore	Julie Meadows	julie.meadows6@nhs.net
Community Hospitals – Malvern / Tenbury	Jenny Biddlecombe	jennybiddlecombe@nhs.net
Community Hospitals - Princess of Wales	Clare Taylor	claire.taylor70@nhs.net
Company Secretary	Maureen Bottrell	**maureenbottrell@nhs.net**
Dental	Rachel Wakely	rachel.wakley@nhs.net
Safeguarding	Abigail Ware	abigail.ware@nhs.net
Sexual Health	Vivien Osborne	vivien.osborne@nhs.net

If you need advice or guidance on the Trust procedures for archiving of records please contact:

Maureen Bottrell, Records Manager, Company Secretary Office

maureenbottrell@nhs.net

Appendix B - Brief Summary of Retention and Disposal Periods for key Trust documents (full version available on intranet http://nww.hacw.nhs.uk/a-z/services/records-management/policies-guidance-and-leaflets/

Type of Record – Health Records	**Minimum Retention Period**	**Notes**
Admission books (where they exist in paper format)	8 years after last entry	Likely to have archival value
Audiology Dietetic and Nutrition District Nursing McMillan (cancer care) Occupational Therapy Physiotherapy Podiatry Speech and Language Therapy	Retain for period of time appropriate to the patient/speciality e.g. children's records should be retained as per the retention period for the records of children and young people; mentally disordered persons (within the meaning of the Mental Health Act 1983) 20 years after the last entry in the record or 8 years after the patient's death if patient died while in the care of the organisation.	Destroy under confidential conditions
Child Health Records (including midwifery, health visiting and school nursing)	Retained until the patients 25th birthday or 26th if young person was 17 at conclusion of treatment, or 8 years after death. If the illness or death could have potential relevance to adult conditions or have genetic implications for the family of the deceased, the advise of clinicians should be sought as to whether to retain the records for a longer period	"
Child Health Records (Notification of visitors/New entrants into a borough either from abroad, or from within the UK from Airports, the Home Office Immigration Centre and the House Options Teams)	Database of notifications – entries should be retained for 2 years. Where a health visitor visits the child the record of the visit should become part of the patient's record and retained until their 25th birthday or 26th if an entry was made when the patient was 17 or 10 years after the patients death if the patient died while in the care of the organisation.	"

Child Protection Register (records relating to)	Retain until patient's 26th birthday or 8 years after the patients death if the patient died while in the care of the organisation.	"
Clinical Audit records	5 years	"
Contraception and Sexual Health Records (Including where a scan is undertaken prior to termination of pregnancy but the patient goes elsewhere for the procedure) Family Planning, and Genito-Urinary Medicine (GUM)	8 years for adults unless there is an implant or device inserted, in which case it is 10 years. All must be reviewed prior to destruction taking into account any serious incident retentions. For clients under 18 retain until patients 25th birthday or 26th if young person was 17 at time of last entry or 8 years after death.	"
Dental, ophthalmic and auditory screening records including orthodontic records and models	10 years. Review and if no longer needed destroy...	"
Diaries – health visitors, district nurses and clinical	3 years from the end of the year to which they relate. Diaries of clinical activity and visits must be written up and transferred to the main patient file. If the information is not transferred the diary must be kept for 8 years.	"
Discharge Books (where they exist in paper format)	8 years after last entry	
Health Visitor records	8 years. Records relating to children should be retained until their 25th birthday or 26th if young person was 17 at time of last entry or 8 years after death. Check for any other involvement that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions.	"
Health records (excluding records not specified elsewhere in this schedule)	8 years after conclusion of treatment or death. Check for any other involvement that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident	"

	retentions.	
Immunisation and vaccination records	For children and young people – retain until the patient's 25th birthday or 26th if the young person was 17 at conclusion of treatment. All others retain for 8 years after conclusion of treatment	"
Learning difficulties – (records of patients with)	20 years after the last entry or 8 years after the patients death if patient died whilst in the care of the organisation	Destroy under confidential conditions
Learning disabilities	20 years after the last entry or 8 years after the patients death if patient died whilst in the care of the organisation	"
Operating theatre registers	10 years after the year to which they relate. Review and consider transfer to a place of deposit.	Likely to have archival value
Out of Hours records (GP cover) including video, DVD and tape voice recordings	If the only record, retain for 8 years. If placed on other records, retain for period appropriate to the specialty. If required in litigation, see Litigation	Destroy under confidential conditions
Outpatients lists (where they exist in paper format)	2 years after the year to which they relate	"
Parent-held records (i.e. records for sick/ill children being cared for at home by community teams NOT the records of new born children. These records are NHS records that belong to clinical staff but which are held by the parent.	At the end of an episode of care the NHS organisation responsible for delivering that care and compiling the record of the care must make appropriate arrangements to retrieve parent-held records. The records should then be retained until the patient's 25th birthday, or 26th if the young person was 17 at the conclusion of the treatment, or 8 years after death	"
Risk Assessment Records	Retain the latest risk assessment until it is superseded	"
		"
Smoking Cessation Records	2 years The Trust should consider whether these records need to be retained for a longer period if any medication etc. is dispensed.	"

Ward registers, including daily bed returns (where they exist in paper format)	2 years after the year to which they relate	
X-ray films (including other image formats for all imaging modalities/diagnostics)	General Patient Records – 8 years after conclusion of treatment Children and young people – until the patients 25th birthday, or if the patient was 17 at the conclusion of treatment until there 26th birthday or 8 years after the patients death if sooner Maternity – 25 years after the birth of the child, including still births Clinical Trials – 15 years after completion of treatment but not more than 20 years. Consider transfer to a place of deposit. Litigation – Records should be reviewed 10 years after the file has been closed and considered for a transfer to a place of deposit.	Guidance from Royal College of Radiologists
X-ray registers (where they exist in paper format)	30 years	Likely to have archival value
X-ray reports (including reports for all imaging modalities)	To be considered as a permanent part of the patient record and should be retained for the appropriate period of time	Destroy under confidential conditions

Type of Record – **Corporate Records**	**Minimum Retention Period**	**Notes**
Accident forms and Register	10 years	Destroy under confidential conditions
Agendas of board meetings, committee, sub-committees (master copies, including associated papers)	Open Board Meetings – Transfer to a Place of Deposit before 20 years as soon as practically possible. Closed Board Meetings – Transfer to a Place of Deposit after 20 years.	FOI exemptions should be noted or duty of confidence indicated
Agendas (other)	2 years	Destroy under confidential conditions
Annual/Corporate reports	3 years, except final annual accounts reports which should be transferred to a Place of Deposit as soon as practically possible with Board Papers.	
Business plans, including local delivery plans	Life of the organisation plus 6 years.	Review and consider transfer to a Place of Deposit
Catering forms	2 years	
Commissioning decisions - appeal documentation	6 years from date of appeal decision	Destroy under confidential conditions
Commissioning decisions - decision documentation	6 years from date of decision	Destroy under confidential conditions
Complaints Correspondence, investigation and outcomes	10 years from completion of action.	Destroy under confidential conditions

Diaries (office)	3 years after the end of the calendar year to which they refer	“
Freedom of Information requests	3 years after closure of the request; 6 years where there has been a subsequent appeal. Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical to keep a summary of the redactions.	Review and destroy under confidential conditions
GMS1 forms (registration with GP)	3 years	“
Health and Safety documentation	6 years	Review and destroy under confidential conditions
History of organisation or predecessors, its organisation and procedures (e.g. establishment order)	Life of organisation plus 6 years.	Review and consider transfer to a Place of Deposit
Incident forms non serious Incident forms - serious	10 years from the date of non-serious incidents 20 years from the date of serious incidents.	Destroy under confidential conditions Consider transfer to a Place of Deposit.
Manuals – policy and procedure (administrative and clinical, strategy documents)	10 years after life of the system (or superseded) to which the policies or procedures refer	Destroy (policies may have archival value)
Meetings and minutes papers of major committees and sub committees (master copies)	Before 20 years but as soon as practically possible.	Transfer to a Place of Deposit
Meetings and minutes papers (other, including reference copies of major committees)	2 years	Destroy under confidential conditions
Papers of minor or short-lived importance not covered elsewhere, e.g.: • Advertising matter • Covering letters • Reminders	2 years after the settlement of the matter to which they relate	“

• Letters making appointments • Anonymous or unintelligible letters • Drafts • Duplicates of documents known to be preserved elsewhere (unless they have important minutes on them) • Indices and registers complied for temporary purposes • Routine reports • Punched cards Other documents that have ceased to be of value on settlement of the matter involved		
Patient Advice and Liaison Service (PALS) Records	10 years after closure of case	Destroy under confidential conditions
Patient information leaflets	6 years after the end of use	Review and consider transfer to a Place of Deposit
Patient Surveys (re access to services)	2 years	Destroy under confidential conditions
Press Releases	6 years	Review and consider transfer to a Place of Deposit
Public Consultations (e.g. about future provisions of services)	5 years after the end of the consultation	Review and consider transfer to a Place of Deposit
Quality and Outcomes Framework (QOF) documents	2 years	“

Quality assurance records (e.g. Healthcare Commission, Audit Commission, King's Fund Organisational Audit, Investors in People)	12 years	Destroy under confidential conditions
Receipts for registered and recorded mail	2 years following the end of the financial year to which they relate	"
Reports (major)	30 years	Likely to have archival value
Requisitions	18 months	Destroy under confidential conditions
Serious incident files	20 years from the date of serious incidents.	Consider transfer to a Place of Deposit.
Subject Access Requests (DPA and AHR) – records of requests	3 years after closure of SAR. 6 years after closure where there has been a subsequent appeal.	Review and destroy under confidential conditions
Time Sheets	2 years	Review and destroy under confidential conditions

Type of Record – **Financial Records**	**Minimum Retention Period**	**Notes**
Accounts – annual (final – one set only)	Transfer to a Place of Deposit as soon as practically possible with Board Papers	Transfer to a Place of Deposit
Accounts – minor records (pass books, paying-in slips, cheque counterfoils, cancelled/discharged cheques (for cheques bearing printed receipts, see Receipts), accounts of petty cash expenditure minor vouchers, duplicate receipt books, income records, laundry lists and receipts)	2 years from completion of audit	
travel and subsistence accounts,	Close of financial year 6 years.	Review and confidentially destroy
Accounts – working papers	3 years from completion of audit	Review and confidentially destroy
Advice notes (payment)	1.5 years	
Audit records – (Internal and external audits) original documents	12 years from completion of audit	Review and confidentially destroy
Audit reports – internal and external (including management letters, value for money reports and systems/final accounts memoranda)	2 years after formal completion by statutory auditor	“
Banks Automated Clearing System (BACS) records	6 years after year end	Review and confidentially destroy
Contracts – financial	Approval files – 15 years, Approved suppliers lists – 11 years	Review and confidentially destroy

Contracts – sealed (and associated records)	Minimum of 6 years, after which they should be reviewed	Review and confidentially destroy
Fraud case files/investigations	6 years (this is also governed by Criminal Appeal legislation and files will need to be kept for longer than 6 years in certain circumstances where there is a criminal prosecution).	Destroy under confidential conditions and in line with NHS CFSMS requirements
Fraud national pro-active exercises	3 years	“
General Medical Services payments	6 years after year end	Review and confidentially destroy
Invoices	6 years after end of financial year to which they relate	Review and confidentially destroy
Payments	6 years after year end	Review and confidentially destroy

Type of Record – **Personnel Records**	**Minimum Retention Period**	**Notes**
Job advertisements	Retain on the personal file of the successful candidate in line with staff record summary retention periods.	Review and confidentially destroy
Job applications (successful)	Keep until 75th birthday, or 6 years after cessation of employment if aged over 75 years at the time	"
Job applications (unsuccessful)	1 year	"
Job descriptions	Retain on the personal file of the successful candidate in line with staff record summary retention periods.	Review and confidentially destroy
Leavers' dossiers (Staff Record Summary)	6 years after individual has left Summary to be retained until individuals 75th birthday, or 6 years after cessation of employment if aged over 75 years at the time.	Review and confidentially destroy
Letters of appointment	6 years after individual has left Summary to be retained until individuals 75th birthday, or 6 years after cessation of employment if aged over 75 years at the time.	Review and confidentially destroy
Pension forms (all)	Although pension information is routinely retained until 100th birthday by the NHS Pensions Agency employers must retain a portion of the staff record until the 75th birthday.	Review and confidentially destroy
Personnel/human resources records – major (e.g. personal files, letters of appointment, contracts, references and related correspondence, registration authority forms, training records, equal opportunity monitoring forms (if retained)	6 years after individual leaves service, at which time a summary of the file must be kept until the individual's 75th birthday Summary should be retained until individuals 75th birthday or until 6 years after cessation of employment if aged over 75 years at the time.	Review and confidentially destroy

Personnel/human resources records – minor (e.g. attendance books, annual leave records, duty rosters, clock cards, turnaround)	2 years	Review and confidentially destroy
Timesheets	2 years	Review and confidentially destroy
Training Records	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The IGA recommends: · **Clinical training records** - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer · **Statutory and mandatory training records** - to be kept for ten years after training completed · **Other training records -** keep for six years after training completed	Review and confidentially destroy

Appendix C – Disposal of Records Template

Box/File number	Records description	Date of Record	Storage Location	Service Delivery Unit / Department	Retention Period	Disposal Date

Signed Departmental Manager	Dated
Signed Senior Manager	Dated

These records have been checked and are authorised for disposal in line with the IICSA Inquiry and the Trust's Records Management Policy.

Appendix D – Retention of Records that pose low or minimal risk to IICSA Inquiry

Record Description	***Recommended Retention Period***
Deceased Patients	• 8 years after the patient has died Minimal risk of the Inquiry reviewing records of deceased patients who are no longer able to consent or provide evidence to Inquiry.
Referrals who have not engaged into treatment	• *2 years after referral* Low risk as no intervention with the Trust has taken place. Referral documentation would be available from the originator source.
Low level interventions with very mild forms of adult mental health treated in a community setting where full recovery is made	• *8 years after discharge* Risk management approach – all records reviewed prior to destruction taking into account any serious incident retentions. Retain if instances of allegations, or investigations, or any records of an institution where abuse has, or may have occurred.
Records with expired retention periods	• Risk management approach – All records reviewed prior to destruction taking into account any serious incident retentions. Retain if instances of allegations, or investigations, or any records of an institution where abuse has, or may have occurred.
Children's records – (including health visiting and school nursing) – 25th or 26th birthday	• 25th birthday or 26th birthday if young person was 17 at conclusion of treatment, or 8 years after death. • Risk management approach – Full child health record reviewed prior to destruction taking into account any serious incident retentions. Retain if instances of allegations, or investigations, or any records of an institution where abuse has, or may have occurred and where patients have accessed adult mental health services. Low risk is attached to partial child health records which usually contain either copy letters or low level interventions which are likely to have taken place. Partial records generally contain copies of letters from other health professionals and low level interventions with patients such as copies of A+E attendance, Domestic Violence copy reports from the Police, low level school nurse interventions. Papers are generally transferred to full child health records if the child had any Child in Need, Child Protection or Looked After Child paperwork.
Sexual Health records	• 8 or 10 years after discharge Risk management approach – all records reviewed prior to destruction taking into account any serious incident retentions. Retain in instances of allegations, or investigations, or any records of any institution where abuse has, or may have occurred.
Pharmacy Team records	• 2 years after drug registers closed or 7 years after records of controlled drug destruction. Low risk as patient record should contain details of the prescription.
General Dental records	• 10 years after discharge Risk management approach – all records reviewed prior to destruction taking into account instances of allegations, or investigations, or any

	records of any institution where abuse has, or may have occurred.
Clinical diaries	• 2 years after year to which they relate if written up and transferred to main patient file, otherwise 8 years Low risk as should be duplication of what is contained in main medical file.
Ward handover sheets	• 2 years after handover Low risk as should be duplication of what is contained in main medical file.
Duty Roster	• 6 years after close of financial year Low risk as payroll / personal file will identify any periods of absences.
Time Sheets	• 2 years Low risk as payroll / personal file information will detail absences.
Finance and Estates records	• destroy as per destruction schedule Low risk.

Appendix E – Retention of Records that pose higher risk to the IICSA Inquiry

Record Description	***Recommended Retention Period***
Patient Advice and Liaison Services (PALs) records	• 10 years after close of financial year High Risk – await more detailed guidance from the IICSA Inquiry before reviewing for destruction.
Complaints / Litigation Files	• 10 years after close of financial year High Risk - await more detailed guidance from the IICSA Inquiry before reviewing for destruction. Retain indefinitely until further guidance
Offender Health - Paper Health Records	• retain indefinitely until further guidance received High Risk - await more detailed guidance from the IICSA Inquiry before reviewing for destruction.
Mental Health Inpatient Records	• retain indefinitely until further guidance received following expiry of 20 year retention period Retention solely for any persons who have been sectioned under the Mental Health Act 1983 must be considerably longer than 20 years where the case may be on-going. High Risk – Full Medical Records for Inpatients Very mild forms of adult mental health treated in a community setting where a full recovery is made may consider treating as an adult records and keep for 8 years after discharge *see appendix 1*
Child Protection / Safeguarding / Statutory Process Records – 25th or 26th birthday of child	• 25th birthday or 26th birthday if young person was 17 at conclusion of treatment, or 8 years after death. High Risk - await more detailed guidance from the IICSA Inquiry before reviewing for destruction. Retain indefinitely until further guidance.