




RECORDS MANAGEMENT POLICY (Electronic and Manual)

Policy number and category	IG04	Information Governance
Version number and date	7	July 2025
Ratifying committee or executive director	Information Governance Steering Group	
Date ratified	August 2025	
Next anticipated review	August 2028	
Executive director	Executive Director of Finance	
Policy lead	Head of Records and Clinical Coding	
Policy author (if different from above)		
Exec Sign off Signature (electronic)		
Disclosable under Freedom of Information Act 2000	Yes	

Policy context

- The Trust recognises that records management is an essential function and that records must be managed throughout their lifecycle, from creation/receipt through to disposal.
- Consistent and accurate recordkeeping underpins the quality of our services, the effectiveness of our decision making, our ability to evidence compliance with legislation and standards, and the efficiency of our staff.
- This policy reflects the Trust's commitment to complying with all applicable legal and regulatory requirements.

Policy requirement (see Section 2)

- Appropriate records will be kept evidencing all activities and transactions of the Trust.
- Records will be organised, managed, and maintained in line with the requirements of this policy to ensure they are accessible by authorised staff when required, and are protected against unauthorised access, accidental loss, and destruction.
- Records will be disposed of systematically in compliance with this policy. Destruction will be complete, secure, authorised, and auditable.

Contents

1.	Introduction	3
1.1.	Rationale	3
1.2.	Scope	3
1.3.	Principles (beliefs):	4
2.	The policy consisting of:	5
3.	The procedure	6
3.1.	Care Records Management (Appendix 4).....	6
3.2.	Personnel File Management (Appendix 2)	7
3.3.	Corporate Records Management (Appendix 3).....	8
4.	Responsibilities	9
5.	Development and Consultation.....	10
6.	Reference documents	10
7.	Bibliography	11
8.	Glossary	12
9.	Audit and assurance.....	19
10.	Appendices	19
	Appendix 1; Equality Analysis Screening Form	20
	Appendix 2; Personnel Records Management Procedures	27
	Appendix 3; Corporate Records Management Procedures.....	29
	Appendix 4; Care Records Management Procedures.....	31

Change Record

Date	Version	Author (Name & Role)	Reasons for review / Changes incorporated	Ratifying Committee
01/07/2025	7	Maria Kane	The Care Records, Corporate Records and Personnel Records policies are all reaching expiry and following an external audit recommendation all 3 policies have been combined with separate procedures for each	IGSG

1. Introduction

1.1. Rationale

Effective records management is fundamental to the operation, accountability, and compliance of the Trust. This policy establishes a comprehensive framework for managing all types of records, including care records, corporate records, and personnel files, ensuring they are accurate, accessible, and secure throughout their lifecycle.

This policy reflects the Trust's commitment to complying with all applicable legal and regulatory requirements, including the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Public Records Acts 1958 and 1967, and NHS Records Management Code of Practice.

1.2. Scope

1.2.1. This policy applies to the management of:

Care Records: Clinical documents relating to service users, including Supplementary Health Records (SHR) and electronic systems like Rio and OnBase.

Personnel Files: Employee records including recruitment, employment-related documentation that the Trust holds in any system including ePersonnel.

Corporate Records: Non-clinical business records, such as administrative logs, minutes, and contracts.

1.2.2. It applies to all formats (paper and electronic), all locations (Trust premises, remote work environments), all services including those hosted by the Trust on behalf of the system (for example LIPI, Meriden and Systemic Family Therapy) and all individuals handling Trust records, including permanent staff, contractors, students/trainees and volunteers.

1.2.3. Examples of records include but are not limited to.

- Post it notes,
- loose papers of any description, registers etc.,
- e-mail,
- Microsoft Teams chats,
- documents held on Microsoft 365,
- microfilms,
- digital dictation recordings,
- video/audio recordings, including Teams videos
- x-rays and other images,
- photographs,
- OnBase,
- TRAC
- registers etc.,

1.2.4. This document sets out a framework within which the staff responsible for managing the Trust's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs

- 1.2.5. For this document, 'care records' applies to the Supplementary Health Record (SHR) of a service user engaged with Birmingham and Solihull Mental Health NHS Foundation Trust. Previous terminology included medical notes, medical records, case notes, and clinical records and health records.
- 1.2.6. For the Trust the primary health record is Rio and for staffs' personal data it is ePersonnel. ePersonnel supplements the electronic information documented in ESR. No clinical or staff information should be held separate to these systems.
- 1.2.7. This document does not include the management of Occupational Health records as these are managed by the service provider and are not shared with the Trust.
- 1.2.8. Please be aware that there are other patient electronic records (EPR) within the Trust, these are IAPTus, used within Birmingham Healthy Minds and the BSol ICB Staff Mental Health Hub, LINKS CarePath (Illy) within the SIAS service, SystemOne is used at HMP Birmingham.
- 1.2.9. For the above services the primary record is their instance of the EPR in use within that Team, although Rio may still be accessed and referenced.
- 1.2.10. Should BHM, SIAS or HMP Birmingham generate paper records they are expected to adhere to this policy for the management of these records.

1.3. Principles (beliefs):

- 1.3.1. The following principles guide the management of all records:

Authenticity: Records must be what they claim to be, created by authorised personnel and appropriately maintained.

Reliability: Records should accurately represent the activities and decisions of the Trust.

Integrity: Records must remain complete and unaltered, protected against unauthorised modification.

Accessibility: Records should only be available to authorised personnel when needed, regardless of format.

Compliance: Records must adhere to statutory and regulatory requirements, including NHS guidelines and data protection laws.

- 1.3.2. Records must be managed throughout their lifecycle, from planning and creation/receipt, through the period of active use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential destruction or archival preservation.

- 1.3.3. It is essential that electronic records are managed throughout their lifecycle as their format renders them susceptible to loss if they are not managed appropriately.

- 1.3.4. The Trust positively supports individuals with learning disabilities and ensures that no-one is prevented from accessing the full range of mental health services available. Staff will work collaboratively with colleagues from learning disabilities services and other organisations, to ensure that service users and carers have a positive episode of care whilst in our services. Information is shared appropriately to support this.

- 1.3.5.** The Trust will treat its staff equitably and reasonably and will not discriminate against individuals or groups based on their ethnic origin, physical or mental abilities, gender, age, religious beliefs, or sexual orientation.
- 1.3.6.** Failure to comply with this policy, for example, unauthorised access or disclosure of personnel identifiable information may lead to disciplinary action being taken and a criminal offence being committed.
- 1.3.7.** If you have any suspicions that fraud or bribery has taken place in relation to the Records Management Policy, please report your concerns as soon as possible. Appropriate contacts can be found on the Trust Counter Fraud and Bribery Intranet pages.
- 1.3.8.** Staff are only permitted to access patient records where a legitimate reason exists, which for the majority for the Trust is for the provision of direct client care. It is not appropriate for staff to access their own medical records, records relating to family members, friends or colleagues. To do so is a breach of confidentiality, please see the [Confidentiality Policy](#), and is both a disciplinary matter and reportable to the ICO (Information Commissioners Office) who can bring a private prosecution against the individual if they feel the incident meets their criteria.

2. The policy consisting of:

This policy provides a framework for the management of records held by the Trust in any format, from creation/receipt, throughout the record lifecycle, until their eventual disposal/ permanent preservation. It ensures that;

- The information we gather is lawful
- That the information is used for a specific and legitimate purpose
- That records are accessible to staff who have a legitimate need
- That records are stored in a secure way to maintain their accuracy and confidentiality
- That records are destroyed when they are no longer required
- That the Trust complies with statutory obligations

3. The procedure

(Please refer to separate procedures for the detailed management of care records, personnel files and corporate records (appendix 1, 2 and 3)):

3.1. Care Records Management ([Appendix 4](#))

Scope: All staff who are recording within the patient record are expected to follow the procedures set out in the [Care Records Management and Procedures](#) document. This includes SHRs, electronic patient records (EPR), and associated documentation, whether in Rio, OnBase, ILLY, IAPTus, SystemOne or other systems.

Processes:

- Staff are expected to write directly into the Progress Notes section of the EPR to maintain a contemporaneous record of ongoing care and treatment. Should jottings be made during a consultation these will be transcribed into the Progress Notes and the jotting 'aide memoir' confidentiality destroyed.
- Any entries made incorrectly or in error, including wrong patient entries, should, under no circumstances, be deleted. Although the entries may not be a true reflection of events/interventions/etc., clinicians will have undoubtedly taken these entries into account when considering risk and care, which needs to be justified and evidenced. See [Care Records Management and Procedures](#) for process in these circumstances.
- Any individual undergoing a pre-registration degree would require their notes to be validated.
- Trainees on post-graduate degree courses (Masters or Doctorate levels) or Assistant psychologists with a first degree in psychology are not required to have all their entries into paper or electronic records validated by a fully registered practitioner i.e. their supervisor. It is the Supervisors' responsibility to ensure that Trainees and Assistants have their notes audited regularly and in line with their experience and competence. Supervisors must ensure that those they supervise are adhering to good practices in reporting clinical and related activities, attending required training and complying with relevant policy.
- Paper Progress Notes are not permitted to be retained, unless they are related to historical paper records that pre-date the EPR and electronic recording
- All loose paper filing is to be sent to the DRM Team based at The Barberry for it to be scanned and filed within OnBase within 10days of receipt.
- The Trust does not allow for information to be scanned and destroyed unless this undertaken by the staff in Digital Records Management (DRM) Team.
- Documentation that is scanned via the DRM Team will be retained for 90days and then confidentially destroyed.
- For staff who are recording in SystemOne, IAPTus or LINKS CarePath (Illy), these systems will be used to document all care and interventions.
- Key IAPTus and Illy documentation will be available to Rio users via the Information From Others Systems (IFOS) interface.
- For staff who are recording on EMIS, this system will be used to document all clinical care and interventions.
- Any Care Record will only be accessed by authorised Trust staff where there is a genuine business need that can be justified if challenged.
- Where records are to be shared with other organisations (e.g. social services and other NHS organisations) this must be done in accordance with documented and agreed information sharing protocols. Refer to the [Confidentiality Policy](#) and [Information Legislation Requests](#) for guidance.
- Any transfer of notes must be done securely. Further information can be obtained from [BSMHFT Safe Haven Guidelines](#).
- Records containing service users' identifiable information can be sent from an NHS.net email address to another NHS.net email address. If there is a requirement

to send identifiable information regarding a service user externally from the Trust this can only be done from a secure account to another secure account (e.g. @pnn.police.uk. Further information can be obtained from [BSMHFT Safe Haven Guidelines](#).

- As a minimum an annual audit of appropriate access to systems will be undertaken in line with Cyber Assurance Framework (CAF) Assessment.

Responsibilities:

- Clinicians must maintain contemporaneous records of care and treatment.
- Information Legalisation Requests (ILR) Team is responsible for the processing of Subject Access Requests (SAR) according to the UK General Data Protection Regulations (UK GDPR) under Article 15 and the Data protection Act 2018 together with Article 16, 17 and 18 UK GDPR, requests for rectification/ erasure and restriction of processing.
- The ILR Team are responsible for processing requests under the Access to Health Records Act which relates to records for deceased service users. Refer to the [Confidentiality Policy](#) and [Information Legislation Requests](#) for further guidance.
- The ILR Team are not responsible for the processing of Subject Access Requests under the Data Protection Act 2018 where litigation against the Trust has been identified, unless directed by the Legal Team to do so. Refer to the [Confidentiality Policy](#) and [Information Legislation Requests](#) for further guidance.
- Records Department staff must ensure compliance with retention and disposal schedules.

3.2. Personnel File Management ([Appendix 2](#))

Scope: Covers all personnel files, including paper files and digital records in the ePersonnel system (<https://onbase.bsmht.nhs.uk/OnBaseWebPRD/Login.aspx>). ePersonnel supplements the electronic information documented in ESR. No current personnel information, from 01 April 2022, is to be stored outside of ePersonnel, and any historical personal information, prior to 01 April 2022, should be filed into the paper personnel file. If this has been scanned, the information needs to be uploaded to ePersonnel.

Processes:

- As from April 2022 all new personnel files must be created in ePersonnel.
- ePersonnel can be accessed via a link on the Trusts intrant's HR pages.
- If line managers have information relating to staff saved locally or in emails this must be saved into ePersonnel and the local copy deleted.
- Any paper personnel files held by Line Managers/ Teams must be scanned and uploaded to ePersonnel by the DRM Team, after which originals are securely disposed.
- Any Personnel record will only be accessed by authorised Trust staff where there is a genuine business need that can be justified if challenged.
- Staff have access to their personnel data held on ePersonnel at any time and do not require speaking to their line manager prior to accessing it
- All paper personnel files will be stored in an appropriate environment that prevents the risk of unauthorised access, accidental loss, destruction, or damage.
- Line Managers will make available open paper personnel files for them to be scanned onto ePersonnel and work with the DRM Team in facilitating this.
- If staff transfer teams within the Trust, ESR must be updated by the current line manager with these updates to ensure the ePersonnel file is available to the new line manager, not doing so could be a breach of confidentiality.
- Closed paper personnel files will be transferred to the Records Department at The Barberry no later than 5 working days from the date the staff member left the Trust.

Responsibilities:

- Line managers are responsible for maintaining personnel files and ensuring that documents are uploaded and saved to ePersonnel only, in a timely manner.
- The HR team must ensure recruitment data is correctly uploaded to ePersonnel from TRAC.
- HR temporary staff team manages the open personnel files of temporary staff on ePersonnel in accordance with this policy
- The DRM Team are responsible for scanning any paper personnel files onto ePersonnel
- The DRM team manages historical paper personnel files for leavers and personnel file management issues in accordance with this policy
- Information Legalisation Requests (ILR) Team is responsible for the processing of Subject Access Requests (SAR) according to the UK General Data Protection Regulations (UK GDPR) under Article 15 and the Data protection Act 2018 together with Article 16, 17 and 18 UK GDPR, requests for rectification/ erasure and restriction of processing. Refer to the [Confidentiality Policy](#) and [Information Legislation Requests](#) for further guidance.
- Records Department staff must ensure compliance with retention and disposal schedules.
- All staff are responsible for Report any concerns fraud or bribery taking place to the Local Counter Fraud specialist, alternatively staff can speak to management or HR regarding any concerns they may have.

3.3. Corporate Records Management ([Appendix 3](#))

Scope: Includes administrative records, such as meeting minutes, contracts, and referral logs and applies to both physical and electronic records, including email records and records created or maintained in information systems such as databases. Corporate Records does not include service user's care record ('health record') nor HR Personnel Files but does cover all other Trust records including those relating to care delivery such as referral logs and ward handover books.

Processes:

- The Trust will create records that serve a clear purpose, providing evidence of the Trust's activities and transactions.
- All records created and received by the Trust during the course of its business will remain the property of the Trust¹.
- Records should be captured in a structured filing system
- The Trust is working towards a position where all corporate records will be captured into a Trust recordkeeping system which is consistent with the requirements of this policy
- Records containing confidential or commercially sensitive information will be protected.
- Vital records will be identified and protected to ensure business continuity in the event of a disaster.
- An Information Asset Owner (IAO) will be responsible for ensuring that specific information assets (systems) are managed and protected appropriately and access controls and retention is applied.
- Records will be retained for as long as is required for operational, legal, audit, and cultural reasons
- Records will be reviewed periodically to ensure they meet operational needs.
- Records will be stored in an appropriate environment, reducing risk of unauthorised access, accidental loss and destruction
- Record destruction will be complete, secure, authorised and auditable.

¹ Staff are not permitted to use corporate records for non-Trust purposes without the approval of their manager. Any staff deemed to have breached this may be subject to disciplinary proceedings.

- Records of historical and administrative importance are identified as being marked for Place of Deposit (DOP) and will be offered and transferred to Birmingham Library upon acceptance.
- Any Corporate record will only be accessed by authorised Trust staff where there is a genuine business need that can be justified if challenged.

Responsibilities:

- Records Department oversees compliance and audits.
- Directors ensure adequate resources for managing records in their domains.
- Records Department staff must ensure compliance with retention and disposal schedules.
- Records Department will develop and maintain guidance and procedures to support staff in the implementation of this policy
- All staff are responsible for Report any concerns fraud or bribery taking place to the Local Counter Fraud specialist, alternatively staff can speak to management or HR regarding any concerns they may have

4. Responsibilities

Post(s)	Responsibilities	Ref
All Staff	Maintain accurate records, handle them securely, and report incidents or breaches.	
Line Managers	Manage team records (e.g., care, personnel files), ensure compliance, and address issues promptly.	
Service, Clinical and Corporate Directors	Ensure appropriate use and sharing of patient and staff identifiable information.	
Workforce Team	Manage care and personnel files and ensure compliance with the Records Management Policy.	
Information Asset Owner (IAO)	Responsible for ensuring that specific information assets (systems) are managed and protected appropriately and access controls and retention is applied.	
Records Staff	To maintain patient and staff records, both in paper and electronically and process Subject Access Requests, in line with National and Trust procedures and with regard to legal requirements.	
Policy Lead	To lead on the development and implementation of the Records Management programme. Develop, maintain and promote guidance and resources to support records management good practice. Provide training and support to staff as required. Liaise with Birmingham Library to arrange the transfer of archives to the library. Complete records audits, escalating any risks identified as required.	

Executive Director	Provide strategic oversight for records management and ensure alignment with Trust goals and national/ legal requirements.	
---------------------------	--	--

5. Development and Consultation

Consultation summary		
Date policy issued for consultation		July 2025
Number of versions produced for consultation		1
Committees / meetings where policy formally discussed		Date(s)
Information Governance Steering Group (IGSG)		05/06/2025
Where received	Summary of feedback	Actions / Response

6. Reference documents

Acts / Regulations

- Access to Health Records Act 1990
- Care Quality Commission: Data Security Review 2016
- Cyber-security Assurance Framework (CAF)
- Data Protection Act 2018
- Department of Health- Operational productivity and performance in English NHS acute hospitals: Unwarranted variations (2016)
- Department of Health, Records Management: NHS Code of Practice for Health and Social Care (DoH 2016).
- Freedom of Information Act 2000
- UK General Data Protection Regulation
- Human Rights Act 1998
- Mental Health Act Code of Practice 2015; Chapter 22 & 27 and AWOL checklist appendix (H)
- NHS England: Five Year Forward View 2014.
- Public Records Acts 1958 and 1967

Related policies and procedures

- Access to Information Policy
- Anti-Fraud Bribery and Corruption Policy
- Corporate Records Management Policy
- Care (health) records management policy
- Confidentiality policy
- Data Quality Policy
- Declarations of Interest Policy
- Disciplinary Policy
- Gender Reassignment Policy
- Information asset owner guidelines

- Information, communications and technology policy
- Information Governance Assurance Policy
- Missing Patient Policy
- Police Intervention Policy
- Recruitment Policy
- Risk Management Policy
- Safe Haven Procedures
- Section 17 Leave Policy
- Trans Equality Policy for Employees
- Whistleblowing Policy

Corporate Records Management Toolkit (https://bsmhftnhsuk.sharepoint.com/sites/connect-bu-ig?fresh_source=copy&creator=fresh#corporate-records-management-toolkit). Guidance referenced in the Policy is as follows:

- Record Creation
 - What information to manage as a Trust record
 - How to name records
 - How to apply version control to records
 - How to protect records against change
- Record Organisation
 - How to design and implement a record file plan
- Record Maintenance
 - How to archive physical records
- Record Disposal
 - Corporate Record Retention Schedule
 - How to dispose records

7. Bibliography

- Audit Commission, Setting the Record Straight, 1995;
- Caldicott Review of Patient Identifiable information, 1997;
- Care Quality Commission Standards
- Department of Health: NHS Confidentiality Code of Practice, 2003;
- Department of Health: Record Management, NHS Code of Practice, 2016
- Ethics Advisory Group Third Party Information and NCRS – initial scoping paper.
- Employment Practices Code of Practice
- Guidance for Access to Health Records Requests under the Data Protection Act.
- HSC 1999/053 'For the Record' – Managing Records in NHS Trusts and Health Authorities.
- ISO15489-1:2001 Information and documentation – Records Management
- Maintaining Good Medical Practice, London GMC 1998.
- Public Records Acts 1958 and 1967.
- National Data Guardian Review of Data Security, Consents and Opt-out (2016) Nursing and Midwifery Council (2005) Guidelines for Record Keeping.

- Nursing and Midwifery Council Guidelines on Documentation and Record Keeping (2002).
- Section 31, Partnership Agreement (2004)

8. Glossary

ACCESS	The availability of, or permission to consult, records. (The National Archives, Records Management Standard RMS1.1).
APPRAISAL	<p>The process of evaluating an organization's activities to determine which records should be kept, and for how long, to meet the needs of the organization, the requirements of Government accountability and the expectations of researchers and other users of the records. (The National Archives, Records Management Standard RMS 1.1).</p> <p>The process of distinguishing records of continuing value from those of no value so that the latter may be eliminated. (The National Archives, Definitions in the Context of the Seamless Flow Programme).</p>
ARCHIVE	<p>Those records that are appraised as having permanent value for evidence of ongoing rights or obligations, for historical or statistical research or as part of the corporate memory of the organization. (The National Archives, Records Management Standard RMS 3.1).</p> <p>It is a legal requirement for NHS records selected as archives to be held in a repository approved by The National Archives; see Place of Deposit below.</p>
AUTHENTICITY	<p>An authentic record is one that can be proven:</p> <ul style="list-style-type: none"> • to be what it purports to be. • to have been created or sent by the person purported to have created or sent it. • to have been created or sent at the time purported. <p>To ensure the authenticity of records, organizations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that record creators are authorized and identifiable and that records are protected against unauthorized addition, deletion, alteration, use and concealment. (BS ISO 15489-1:2016(en)).</p>
CLASSIFICATION	The systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system. (BS ISO 15489-1:20016(en)).

CONVERSION (SEE ALSO MIGRATION)	The process of changing records from one medium to another, or from one format to another. (BS ISO 15489-1:2016(en)).
CORPORATE RECORDS	Records (other than health and personnel records) that are of, or relating to, an organisation's business activities covering all the functions, processes, activities and transactions of the organisation and of its employees.
CURRENT RECORDS	Any record necessary for conducting the current and ongoing business of an organisation.
DESTRUCTION	The process of eliminating or deleting records beyond any possible reconstruction. (BS ISO 15489-1:2016(en)).
DISPOSAL	Disposal is the implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive institution). They may also include the movement of records from one system to another (for example, paper to electronic). (The National Archives, Records Management Standard RMS1.1).
DISPOSITION	A range of processes associated with implementing records retention, destruction or transfer decisions, which are documented in disposition authorities or other instruments. (BS ISO 15489-1:2016(en)).
ELECTRONIC RECORD MANAGEMENT SYSTEM	A system that manages electronic records throughout their lifecycle, from creation and capture through to their disposal or permanent retention, and which retains their integrity and authenticity while ensuring that they remain accessible. (The National Archives, Definitions in the Context of the Seamless Flow Programme).
FILE	An organised unit of documents grouped together either for current use by the creator or in the process of archival arrangement, because they relate to the same subject, activity or transaction. A file is usually the basic unit within a records series.
FILING SYSTEM	A plan for organising records so that they can be found when needed. (The National Archives, Records Management Standard RMS 1.1).
HEALTH RECORDS	A single record with a unique identifier containing information relating to the physical or mental health of a given patient who can be identified from that information, and which has been recorded by, or on behalf of, a health professional, in connection with the care of that patient. This may comprise text, sound, image and/or paper and must contain sufficient information to support the diagnosis, justify the treatment and facilitate the ongoing care of the patient to whom it refers.

INDEXING	The process of establishing access points to facilitate retrieval of records and/or information. (BS ISO 15489-1:2016(en)).
INFORMATION ASSET OWNER	A designated individual within an organisation who is responsible for ensuring that specific information assets are managed and protected appropriately. These assets can include data, documents, systems, or databases that are critical to the organisation's operations
INFORMATION AUDIT	An information audit looks at how an information survey will be carried out and what the survey is intended to capture.
INFORMATION COMMISSIONER	The Information Commissioner enforces and oversees the Data Protection Act 2018 and the Freedom of Information Act 2000.
INTEGRITY OF RECORDS	The integrity of a record refers to its being complete and unaltered. It is necessary that a record be protected against unauthorised alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorised and who is authorised to make them. Any unauthorised annotation, addition or deletion to a record should be explicitly identifiable and traceable
INFORMATION SURVEY/ RECORDS AUDIT	<p>A comprehensive gathering of information about records created or processed by an organisation. (The National Archives, Records Management Standards and Guidance – Introduction Standards for the Management of Government Records) It helps an organisation to promote control over its records and provides valuable data for developing records appraisal and disposal procedures. It will also help to:</p> <p>Identify where and when health and other records are generated and stored within the organisation and how they are ultimately archived and/or disposed of.</p> <p>Accurately chart the current situation in respect of records storage and retention organization-wide, to make recommendations on the way forward and the resource implications to meet existing and future demands of the records management function.</p>
JOINTLY HELD RECORDS	A record held jointly by health and social care professionals, for example in a Mental Health and Social Care Trust. A jointly held record should be retained for the longest period for that type of record, i.e. if social care has a longer retention period than health, the record should be held for the longer period.
MICROFORM	Records in the form of microfilm or microfiche, including aperture cards

MIGRATION (ALSO SEE CONVERSION)	The act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability. (BS ISO 15489-1:2016(en)).
MINUTES (MASTER COPIES)	Master copies are the copies held by the secretariat of the meeting, i.e. the person or department who takes, writes and issues the minutes
MINUTES (REFERENCE COPIES)	Copies of minutes held by individual attendees at a given meeting
NHS CARE RECORDS SERVICE	The NHS Care Records Service (NHS CRS) will connect all GPs, acute, community and mental health NHS trusts in a single, secure national system that will enable individual electronic patient record details to be accessed by authorized personnel, at the appropriate level, anywhere in England, via use of a unique identifier. The unique identifier to be employed throughout the NHS and its associated systems is the NHS number.
NHS NUMBER	<p>Introduced in 1996, the NHS number is a unique 10-character number assigned to every individual registered with the NHS in England (and Wales). The first nine characters are the identifier, and the tenth is a check digit used to confirm the number's validity. Babies born in England and Wales are allocated an NHS number by Maternity Units, at the point of Statutory Birth Notification.</p> <p>The NHS number is used as the common identifier for patients across different NHS organizations and is a key component in the implementation of the NHS CRS.</p>
NHS RECORDS (PUBLIC RECORDS ACT)	All NHS records are public records under the terms of the Public Records Act 1958 sections 3(1)–(2). All records created and used by NHS employees are public records.
PAPER RECORDS	Records in the form of files, volumes, folders, bundles, maps, plans, charts, etc
PERMANENT RETENTION	Records may not ordinarily be retained for more than 20 years. However, the Public Records Act provides for records, which are still in current use to be legally retained. Additionally, under separate legislation, records may need to be retained for longer than 20 years, for example Occupational Health Records relating to the COSHH(Control of Substances Hazardous to Health) Regulations, or records required for variant CJD surveillance.
PERSONAL DATA	Data which relates to a living individual who can be identified from that data or from data and from other information, which is in the possession of, or is likely to come into the possession of the data controller (e.g. our Trust) (Data Protection Act 2018).

PLACE OF DEPOSIT	<p>A record office, which has been approved for the deposit of public records in accordance with section 4(1) of the Public Records Act 1958. This is usually the record office of the relevant (i.e. county, borough, or unitary) local authority. A list of those repositories recognized by The National Archives for the deposit of NHS archives is in Annex E. Contact details for them are to be found in the ARCHON directory on its website:</p> <p>http://discovery.nationalarchives.gov.uk/find-an-archive</p> <p>An organisation wishing to have records preserved as archives should consult with The National Archives in the first instance, unless that organisation has an existing working relationship with an approved Place of Deposit.</p> <p>Some individual hospitals have themselves been appointed as a Place of Deposit. In practice, these have tended to be those larger hospitals, which can commit the resources necessary to provide appropriate conditions of storage and access and to place them under the care of a professionally qualified archivist. The National Archives can provide advice to any organization wishing to apply for Place of Deposit status. Further information about the work of archivists in NHS Trusts is available from the Health Archives Group</p>
PRESENTATION	The transfer to a third party (for example a University) of public records which have been rejected by The National Archives, but which are not destroyed, under section 3(6) of the Public Records Act 1958
PRESERVATION	Processes and operations involved in ensuring the technical and intellectual survival of authentic records through time. (BS ISO 15489-1:2016(en)).
PROTECTIVE MARKING	The process of determining security and privacy restrictions on records.
PUBLICATION SCHEME	A publication scheme is required of all NHS organizations under the Freedom of Information Act. It details information, which is available to the public now or will be in the future, where it can be obtained from and the format it is or will be available in. Schemes must be approved by the Information Commissioner and reviewed periodically to make sure they are accurate and up to date
PUBLIC RECORDS	<p>Records as defined in the Public Records Act 1958 or subsequently determined as public records by The National Archives.</p> <p>Records of NHS organisations (and those of predecessor bodies to NHS organizations) are defined as public records under the terms of the Public Records Act 1958 sections 3(1)–(2). NHS records are not owned by the NHS organization that created them and may not be</p>

	<p>retained for longer than 20 years without formal approval by The National Archives, (The National Archives).</p> <p>Records of services supplied within NHS organisations but by outside contractors are not defined as public records, but are subject to the Freedom of Information Act</p>
PUBLIC RECORDS ACT 1958	<p>For further information, including the text of the Act, see The National Archives' website:</p> <p>www.nationalarchives.gov.uk/policy/act</p>
RECORDS	<p>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. (BS ISO 15489.1).</p> <p>An NHS record is anything, which contains information (in any media), which has been created or gathered as a result of any aspect of the work of NHS employees – including consultants, agency or casual staff</p>
RECORDS MANAGEMENT	<p>Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. (BS ISO 15489-1:2016(en)).</p>
RECORDS SERIES	<p>A series is the main grouping of records with a common function or subject – formerly known as 'class'. (The National Archives)</p> <p>Documents arranged in accordance with a filing system or maintained as a unit because they result from the same accumulation or filing process, or the same activity, because they have a particular form, or because of some other relationship arising out of their creation, receipt or use. (International Council on Archives' (ICA) General International Standard Archival Description or ISAD(G)).</p> <p>Terminology International Council on Archives (ica.org)</p> <p>A series comprises the record of all the activities that are instances of a single process. A series may be large or small: it is distinguished not by its size, but by the fact that it provides evidence of a particular process. If an activity takes place that is unique, rather than an instance of a process, its records form a series in their own right. (Elizabeth Shepherd and Geoffrey Yeo, Managing Records: a handbook of principles and practice (Facet 2003).</p>
RECORD SYSTEM/ RECORD KEEPING SYSTEM	<p>An information system, which captures, manages and provides access to records through time. (The National Archives, Records Management: Standards and Guidance – Introduction Standards for the Management of Government Records).</p> <p>Records created by the organisation should be arranged in a record-keeping system that will enable the organisation to obtain the</p>

	<p>maximum benefit from the quick and easy retrieval of information. Record-keeping systems should contain descriptive and technical documentation to enable the system and the records to be understood and to be operated efficiently, and to provide an administrative context for effective management of the records, including a documented set of rules for referencing, titling, indexing and, if appropriate, the protective marking of records.</p> <p>These should be easily understood to enable the efficient retrieval of information and to maintain security and confidentiality.</p>
REDACTION	The process of removing, withholding or hiding parts of a record due to either the application of a Freedom of Information Act or Data Protection Act exemption or a decision by The National Archives to restrict access where sensitivity, copyright or data protection issues arise. (The National Archives, Definitions in the Context of the Seamless Flow Programme).
REGISTRATION	Registration is the act of giving a record a unique identifier on its entry into a record- keeping system e.g. ESR number, NHS number.
RETENTION	The continued storage and maintenance of records for as long as they are required by the creating or holding organisation until their eventual disposal, according to their administrative, legal, financial and historical evaluation
REVIEW	The examination of records to determine whether they should be destroyed, retained for a further period, transferred to an archival establishment, or presented to a third party (for example a university).
TRUST FILE PLAN	The Trust file plan is a classification scheme which enables which enables records to be categorised in systematic and consistent manner to facilitate their capture, retrieval, maintenance and disposal.
SATELLITE BASES	BSMHFT premises which act as satellite to a specified home base. All Records staff will have responsibility for promoting good record keeping across its satellite bases.
VITAL RECORDS	Vital records are records without which the organisation could not function. They are essential records that are necessary to document and protect corporate assets, obligations and resources of the Trust.
SUPPLEMENTARY HEALTH RECORD	A paper care record that is used in conjunction with electronic patient record to store documents; that cannot be captured directly into the electronic record, that have been scanned into the electronic record but need to be retained for legal reasons, for information that is received in paper format from external sources for example service users, external healthcare providers and local government agencies.

TRACKING	Creating, capturing and maintaining information about the movement and use of records, (BS ISO 15489-1:2001(E)).
TRANSFER OF RECORDS	<p>Transfer (custody) – Change of custody, ownership and/or responsibility for records, (BS ISO 15489-1:2016(en)).</p> <p>Transfer (movement) – Moving records from one location to another, (BS ISO 15489- 1:2016(en)).</p> <p>Records identified as more appropriately held, as archives should be offered to our The National Archives, place of deposit, who will decide regarding their long-term preservation.</p>
VITAL RECORDS	Vital records are records without which the organisation could not function. They are essential records that are necessary to document and protect corporate assets, obligations and resources of the Trust.
WEEDING	The process of removing inactive/non-current health records from the active/current or primary records storage area to a designated secondary storage area after a locally agreed timescale after the date of last entry in the record

9. Audit and assurance

Element to be monitored	Lead	Tool	Frequency	Reporting Arrangements	Acting on Recommendations and Lead
Management of electronic records – system and controls	Deputy Head of Records	External Audit	Annual	Information Governance Steering Group (IGSG)	Head of Records and Clinical Coding
Management of physical corporate records –controls, retention, disposal	Deputy Head of Records	External Audit	Annual	Information Governance Steering Group (IGSG)	Head of Records and Clinical Coding
Cyber-Security Assurance Framework (CAF)	Head of Records and Clinical Coding	Final external Audit Reports and Polices	Annual	Information Governance Steering Group (IGSG)	Head of Records and Clinical Coding
Line manager compliance with no local personnel files	Deputy Head of Records	Physical site checks	Annual	Information Governance Steering Group (IGSG)	Head of Records and Clinical Coding
Line manager compliance with closed file transfer requirements	Deputy Head of Records	Physical site checks	Annual	Information Governance Steering Group (IGSG)	Head of Records and Clinical Coding
Ensure the Trust's procedures and policies are being following in relation to the retention and safeguarding of personnel files.	Local Counter Fraud Specialist	Audit report	Periodically	Information Governance Steering Group (IGSG)	Local Counter Fraud Specialist

10. Appendices

Appendix 1; Equality Analysis Screening Form

A word version of this document can be found on the HR support pages on Connect

<http://connect/corporate/humanresources/managementsupport/Pages/default.aspx>

Title of Policy	Records Management Policy		
Person Completing this policy	Maria Kane	Role or title	Head of Records and Clinical Coding
Division	Corporate	Service Area	Records
Date Started	12/05/2025	Date completed	
Main purpose and aims of the policy and how it fits in with the wider strategic aims and objectives of the organisation.			
<p>The Trust recognises that records are a valuable resource and an important business asset. Effective management of records will support the Trust's activities and decision making, as well as ensuring accountability to stakeholders. The benefits of managing corporate records in a consistent and controlled manner include:</p> <ul style="list-style-type: none">• Control the creation and growth of records.• Faster information retrieval, enabling increased productivity.• Consistency and efficiency of administration and elimination of duplication resulting in savings in both staff time and storage.• Opportunity for more evidence based decision making as records are more easily located.• Evidence of organisational activity for regulatory compliance and in the event of litigation, protecting the interests of the Trust and supporting the rights of stakeholders.• Identification and protection of vital records to ensure business continuity in the event of a disaster. <p>Preservation of a corporate memory, preventing the loss of valuable information when staff leave the Trust. BSMHFT creates public records as defined in the Public Records Acts of 1958 and 1967 and is required by law to manage its records in accordance with its legal and regulatory environment. The Department of Health outlines the standards required for the management of NHS records in the 'Records Management: NHS Code of Practice' and compliance is monitored via the Data Security and Protection Toolkit.</p>			

Who will benefit from the proposal?	
The policy is Trust wide and applies to all staff members, whether permanent or temporary. This includes contractors, apprentices, volunteers and placements in the course of their work for and on behalf of the Trust, whether working directly for the Trust or in partnership with it. Staff, contractors, apprentices, volunteers will benefit by having clear guidance on how corporate records should be managed and maintained and their roles and responsibilities	
Does the policy affect service users, employees or the wider community? <i>Add any data you have on the groups affected split by Protected characteristic in the boxes below. Highlight how you have used the data to reduce any noted inequalities going forward</i>	
No	
Does the policy significantly affect service delivery, business processes or policy? <i>How will these reduce inequality?</i>	
No	
Does it involve a significant commitment of resources? <i>How will these reduce inequality?</i>	
No	
Does the policy relate to an area where there are known inequalities? (e.g. seclusion, accessibility, recruitment & progression)	
No	
Impacts on different Personal Protected Characteristics – Helpful Questions:	
<i>Does this policy promote equality of opportunity?</i> <i>Eliminate discrimination?</i> <i>Eliminate harassment?</i> <i>Eliminate victimisation?</i>	<i>Promote good community relations?</i> <i>Promote positive attitudes towards disabled people?</i> <i>Consider more favourable treatment of disabled people?</i> <i>Promote involvement and consultation?</i> <i>Protect and promote human rights?</i>
Please click in the relevant impact box and include relevant data	

Personal Protected Characteristic	No/Minimum Impact	Negative Impact	Positive Impact	Please list details or evidence of why there might be a positive, negative or no impact on protected characteristics.
Age			x	Policy reflects the need to accurately record a patient's information. The Insight report at 01/07/2025 for current patients advises the following: Age 85 plus – 3232 Age 75-84 – 5010 Age 65-74 – 4591 Age 55-64 – 7327 Age 45-54 – 9075 Age 35-44 – 12152 Age 25-34 – 12765 Age 16-24 – 3928 Age 16 and below - 2198
Including children and people over 65 Is it easy for someone of any age to find out about your service or access your policy? Are you able to justify the legal or lawful reasons when your service excludes certain age groups				
Disability			x	Policy reflects the need to accurately record a patient's information. The Insight report at 01/07/2025 for current patients advises the following: Disability – 2036 Not known - 58242
Including those with physical or sensory impairments, those with learning disabilities and those with mental health issues Do you currently monitor who has a disability so that you know how well your service is being used by people with a disability? Are you making reasonable adjustment to meet the needs of the staff, service users, carers and families?				
Gender			x	Policy reflects the need to accurately record a patient's preferred gender in that the electronic record allows for the choice of female, male, non-binary and unknown. The Insight report at 01/07/2025 for current patients advises the following choices: Female – 34,335 Male – 25,875 Non binary – 54 Not stated – 1 Other – 1

				Unknown - 12
<p>This can include male and female or someone who has completed the gender reassignment process from one sex to another</p> <p>Do you have flexible working arrangements for either sex?</p> <p>Is it easier for either men or women to access your policy?</p>				
Marriage or Civil Partnerships	X			
<p>People who are in a Civil Partnerships must be treated equally to married couples on a wide range of legal matters</p> <p>Are the documents and information provided for your service reflecting the appropriate terminology for marriage and civil partnerships?</p>				
Pregnancy or Maternity	X			
<p>This includes women having a baby and women just after they have had a baby</p> <p>Does your service accommodate the needs of expectant and post natal mothers both as staff and service users?</p> <p>Can your service treat staff and patients with dignity and respect relation in to pregnancy and maternity?</p>				
Race or Ethnicity			x	<p>Policy reflects the need to accurately record a patient's information. The Insight report at 01/07/2025 for current patients advises the following:</p> <p>White – 34645</p> <p>Asian/Asian British – 10878</p> <p>Black/Black British – 4558</p> <p>Mixed – 3012</p> <p>Not known – 2833</p> <p>Not stated – 2365</p> <p>Other - 1987</p>
<p>Including Gypsy or Roma people, Irish people, those of mixed heritage, asylum seekers and refugees</p> <p>What training does staff have to respond to the cultural needs of different ethnic groups?</p> <p>What arrangements are in place to communicate with people who do not have English as a first language?</p>				
Religion or Belief			x	<p>Policy reflects the need to accurately record a patient's information. The Insight report at 01/07/2025 for current patients advises the following:</p> <p>Unknown – 47,548</p> <p>Christian – 6516</p> <p>Muslim – 2471</p>

				None – 2257 Not stated – 621 Other – 336 Sikh – 306 Hindu – 148 Buddhist – 42 Jewish - 33
Including humanists and non-believers Is there easy access to a prayer or quiet room to your service delivery area? When organising events – Do you take necessary steps to make sure that spiritual requirements are met?				
Sexual Orientation			x	The policy supports all sexual orientations. The Insight report at 01/07/2025 for current patients advises the following choices: Unknown – 46,973 Heterosexual/Straight – 7947 Heterosexual – 3590 No stated – 565 Bisexual – 375 Declined to disclose – 258 Gay/Lesbian – 230 Other – 132 Gay (Male) – 81 Lesbian – 81 Uncertain – 38 Pansexual – 28 Sexually attracted to neither male nor female - 16
Including gay men, lesbians and bisexual people Does your service use visual images that could be people from any background or are the images mainly heterosexual couples? Does staff in your workplace feel comfortable about being 'out' or would office culture make them feel this might not be a good idea?				
Transgender or Gender Reassignment			x	Policy reflects the need to accurately record a patient's preferred gender The Insight report at 01/07/2025 for current patients advises the following: Transgender - 9
This will include people who are in the process of or in a care pathway changing from one gender to another Have you considered the possible needs of transgender staff and service users in the development of your policy or service?				

Human Rights	X			
Affecting someone's right to Life, Dignity and Respect?				
Caring for other people or protecting them from danger?				
The detention of an individual inadvertently or placing someone in a humiliating situation or position?				
If a negative or disproportionate impact has been identified in any of the key areas would this difference be illegal / unlawful? I.e. Would it be discriminatory under anti-discrimination legislation. (The Equality Act 2010, Human Rights Act 1998)				
	Yes	No		
What do you consider the level of negative impact to be?	High Impact	Medium Impact	Low Impact	No Impact
				X
If the impact could be discriminatory in law, please contact the Equality and Diversity Lead immediately to determine the next course of action. If the negative impact is high a Full Equality Analysis will be required.				
If you are unsure how to answer the above questions, or if you have assessed the impact as medium, please seek further guidance from the Equality and Diversity Lead before proceeding.				
If the policy does not have a negative impact or the impact is considered low, reasonable or justifiable, then please complete the rest of the form below with any required redial actions, and forward to the Equality and Diversity Lead .				
Action Planning:				
How could you minimise or remove any negative impact identified even if this is of low significance?				
No negative impact identified, however review policy and procedures at regularly to maintain standards				
How will any impact or planned actions be monitored and reviewed?				
Review yearly and update any adhoc amendments required				
How will you promote equal opportunity and advance equality by sharing good practice to have a positive impact other people as a result of their personal protected characteristic.				
Through the involvement of all in the development and review of the policy and audit results.				

Please save and keep one copy and then send a copy with a copy of the policy to the Senior Equality and Diversity Lead at bsmhft.edi.queries@nhs.net. The results will then be published on the Trust's website. Please ensure that any resulting actions are incorporated into Divisional or Service planning and monitored on a regular basis

Appendix 2; Personnel Records Management Procedures

1. File Creation – New Starters (inc. Re-employed Leavers)

- 1.1. An ePersonnel file will be created when a new staff member has been assigned to their team.
- 1.2. When a staff member has successfully completed the recruitment process, the HR recruitment team will transfer personnel file documents from TRAC to ePersonnel no later than 2 working days after staff start date.

2. ePersonnel File Organisation

- 2.1. Records that required to be stored on a personnel file will be uploaded to ePersonnel on a regular basis no later than 2 working days after the date of creation. ePersonnel can be accessed via <https://onbase.bsmht.nhs.uk/OnBaseWebPRD/Login.aspx>
- 2.2. Records must not be stored on Home Drives or Team Drives. The Trust only approves storage of personal information on ePersonnel from April 2022 or on a paper personnel file prior to this date.
- 2.3. Records will be arranged in ePersonnel according to the document type/ category.

3. Paper Personnel File Storage

- 3.1. Personnel files will be stored in a location and manner so they can be easily located and retrieved by authorised staff.
- 3.2. All practicable measures will be in place to ensure personnel files are stored in a secure environment that protects them from unauthorised access and other risks that might lead to inadvertent damage or loss at all times. As a minimum, open personnel files will be stored in lockable cabinets and a record of all current key holders maintained.
- 3.3. Personnel files will be stored in an environment that complies with the Trust's health and safety policy.

4. Paper Personnel File Tracking

- 4.1. The line manager and recipient are responsible for ensuring that a record confirming the transfer and receipt of a personnel file is created whenever an open personnel file is transferred:
 - To a new line manager.
 - Between different site locations including non-Trust sites.
 - To another service area within the same site location.
- 4.2. The line manager is responsible for ensuring that a record confirming the transfer and receipt of a personnel file is retained on the personnel file.
- 4.3. Any issues arising from tracking, for example, recipient has not confirmed receipt within reasonable period, must be reported to the Records Department.

5. File Transportation (paper and electronic)

- 5.1. The only accepted method of transferring paper personnel files between site locations will be in a:-
 - blue plastic holdall (for transporting several files)
 - blue plastic pouch (for transporting 1-3 files)
 - grey tamper proof self-seal envelop (for transporting 1-3 files).
- 5.2. The secure transfer bags/boxes used to transport paper personnel files internally will be clearly labelled as follows:-
 - Recipient name and role in full
 - Site name and team
 - State 'internal post' in the top right of the package
 - State senders name and location in the top left of the package
- 5.3. All copies of ePersonnel files transported externally will only be sent via secure transfer

for example a Secure FTPS or Egress. Before any transfer can take place staff need to advise Information Governance so a transfer method can be agreed.

6. Closed Paper Personnel Files Management (Archiving, Access & Disposal)

- 6.1. Closed physical personnel files will be transferred to the Records Department at the Barberry no later than 5 working days from the date the staff member has left service with the Trust. Files should be transferred as per the previous section and addressed to Records Department, The Barberry, 25 Vincent Drive, Birmingham B15 2FG
- 6.2. The Records Department will transfer closed personnel files to the Trust's approved off-site storage provider in accordance with the Corporate Records Management procedures signed off by the Trust's Senior Information Risk Officer (SIRO).
- 6.3. A request from a staff member to access a closed personnel file will be sent to Records Management and processed in accordance with the Corporate Records Management procedures signed off by the Trust's SIRO.
- 6.4. A closed personnel file sent to a staff member will be returned to Records Management as soon as the task has been completed. The movement of the file will be tracked in accordance with [section 4. Paper Personnel File Tracking](#).
- 6.5. Closed personnel files will be retained for a minimum of 6 years from the end of the calendar year in which the contract was terminated and then reviewed for disposal in accordance with the Corporate Records Management procedures signed off by the Trust's SIRO
- 6.6. Personnel files will not be destroyed if there is a legal or cultural reason as defined in the Corporate Records Management procedures signed off by the Trust's SIRO.
- 6.7. The disposal of closed personnel files will be carried out by Records Management in a confidential, secure, and auditable manner in accordance with the Corporate Records Management procedures signed off by the Trust's SIRO.

7. Home Working

- 7.1. Physical personnel files will only be taken home in exceptional circumstances and where there is a genuine business need. The movement of the file will be tracked – [see section 4. Paper Personnel File Tracking](#)
- 7.2. Personnel files will be stored and transported securely until returned to the site location – [see section 5. File Transportation](#). Under no circumstances will personnel files be left unsupervised in vehicles or in public spaces at any time.
- 7.3. Personnel files will be returned to the Trust premises as soon as possible and no later than the next calendar day. If a staff member is on sick leave for more than 2 days, then arrangements must be made to return the personnel file to the site location.

Appendix 3; Corporate Records Management Procedures

1. The Corporate Records Management (CRM) Toolkit

- 1.1 Is available on Connect to support staff in the implementation of this policy and the development of department / service specific procedures for recordkeeping where appropriate.

2. Management of Records

- 2.1. Until the trust wide recordkeeping system is in place, records will be managed at department / service level.

3. Records creation

- 3.1. Complete, authentic, and reliable records should be kept where there is a requirement to evidence a business decision or transaction. See the [CRM Toolkit](#) for guidance.
- 3.2. Records will be named and indexed in a consistent and logical manner. See the [CRM Toolkit](#) for best practice guidance Version control will be applied to documents that go through multiple versions or are collaborated on by a number of staff before a final version of the record is created.
- 3.3. Guidance on the correct use of version control is available in the [CRM Toolkit](#).
- 3.4. Multiple copies of records should not be kept unless necessary. Where multiple copies exist, the copy held by the department / service which created the record or received the record where a record is created externally to the Trust, will be the record copy. Papers for committees / meetings will be owned by the convenor of the meeting.
- 3.5. Records will be created or captured in a format or manner that reduces the risk of staff accidentally altering or making a change to a record. See the [CRM Toolkit](#) for guidance.
- 3.6. Records of a confidential or commercially sensitive nature will be protectively marked to clearly indicate the sensitivity of the information they contain. Guidance is available in the [CRM Toolkit](#).

4. Records transfer

- 4.1. Records must be appropriately protected when being transferred or taken offsite. Safe Haven procedures should be followed.

5. Records maintenance

- 5.1. All corporate records will be kept securely in shared network drives or information systems where they are in electronic format. Or in an appropriately secure environment such as in locked cabinets or rooms where they are in a physical format, until the Trust recordkeeping system is confirmed and then records will be captured into this.
- 5.2. All Privilege Accounts will be secured and access audited.
- 5.3. Records should be retained for the retention period defined in the [Corporate Record Retention Schedule](#).
- 5.4. Physical records which are no longer consulted frequently may be transferred to the Trust's off site storage provider for the remainder of their retention period. Ownership will remain with the originating department / service. See the [CRM Toolkit](#) for guidance.
- 5.5. Where services are transferred to a third party and records are required for the ongoing functioning of that service, copies of records necessary for the continuation of that service may be provided to the third party. Originals will be retained by the Trust in compliance with the Corporate Record Retention Schedule.
- 5.6. Where services move / close the department / service will nominate an individual to lead on corporate records management for the move/closure. Appropriate steps should be taken to ensure the records associated with that service are managed in line with this policy.
- 5.7. Where any records or filing is found for personnel files, an eclipse needs to be raised by the finder before the file or filing is processed to allow for transparency for any access to records requests

6. Records disposal

- 6.1. Each department / service should have a regular (usually annual) programme of records disposal.
- 6.2. Records should be reviewed once the retention period has been reached. The review should consider the ongoing value of the records, resulting in one of the following actions:
- 6.3. Retain for a further specified period, where records still have business value, or are required for audit or legal purposes. Where records are subject to a legal hold, this action must be taken.
- 6.4. Confidential destruction, where records have no further value. Where multiple copies exist, all copies should be destroyed.
- 6.5. Retain as archives, where records are identified as having historical and administrative importance. Such records should be transferred to the Corporate Records Management Officer who will offer the records for transfer to Birmingham Library.
- 6.6. Disposal decisions should be documented via the Record Destruction Form and destruction of records must be authorised by an appropriate manager. This form shall then be sent to the Corporate Records Management Officer. See the [CRM Toolkit](#) for guidance and for a copy of the form.

7. Training

- 7.1. The Corporate Records Management Officer will develop and maintain guidance and procedures to support staff in the implementation of this policy.

Appendix 4; Care Records Management Procedures

[CareRecordsProceduresV7.doc](#)