NHS
Nottingham and Nottinghamshire
Clinical Commissioning Group

Records Management Policy

2021-2024

Version:	2.0
Approved by:	Information Governance Steering Group
Date approved:	April 2021
Date of issue (communicated to staff):	May 2021
Next review date:	April 2024
Document authors:	Head of Corporate Assurance; Head of Information Governance

CONTROL RECORD				
Reference Number IG-006	**Version** 2.0	**Status** Final	**Authors** Head of Corporate Assurance; Head of Information Assurance	
			Sponsor Associate Director of Governance	
			Team Corporate Assurance Team	
Title	Records Management Policy			
Amendments	Retention Schedule was strengthened, in line with NHS England Retention Schedule			
Purpose	This Policy sets out the approach taken within the CCG to provide a robust records management system for the management of corporate information			
Superseded Documents	Records Management Policy v1.0			
Audience	All employees of NHS Nottingham and Nottinghamshire CCG (including those working within the organisation in a temporary capacity)			
Consulted with	Information Governance Steering Group			
Equality Impact Assessment	Complete – see Section 16			
Approving Body	Information Governance Steering Group		**Date approved**	April 2021
Date of Issue	May 2021			
Review Date	April 2024			
This is a controlled document and whilst this policy may be printed, the electronic version available on the CCG's document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.				

Nottingham and Nottinghamshire CCG's policies can be made available on request in a range of languages, large print, Braille, audio, electronic and other accessible formats from the Engagement and Communications Team at nnccg.team.communications@nhs.net

Contents

1. Introduction

1.1. Records management is the process by which Nottingham and Nottinghamshire CCG (hereafter referred to as 'the CCG') manages all aspects of its record keeping, whether internally or externally generated, and in any format or media type, from their creation, all the way through their lifecycle and to their eventual destruction.

1.2. The CCG is dependent on its documents and records to operate efficiently and account for its actions. Information is a corporate asset and the CCG's records are important sources of administrative, evidential and historical information. They are vital to the CCG to support current and future operations, for the purposes of accountability and transparency, and for an awareness and understanding of its history and procedures.

1.3. The CCG has a statutory obligation under the Data Protection Act 2018, General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000, to maintain accurate records of its activities and to make arrangements for their safekeeping and secure disposal. All records created in the course of CCG business are public records under the terms of the Public Records Act 1958.

1.4. In addition, all NHS organisations are required to work to the standards set out within the Information Governance Alliance (IGA) Records Management Code of Practice for Health and Social Care Act 2016.

1.5. This policy relates to all records held in any format or media by the CCG, including corporate and health records. Records should be classified as sensitive or non-sensitive in terms of their impact on the running of the business if lost or disclosed.

- **Corporate records** (non-clinical) provide evidence of actions and decisions and represent a vital asset to support daily functions, operations, audit and legal requirements. Records support policy formation and managerial decision-making, protect the interests of the organisation, staff and our population. Records support consistency, continuity, efficiency and productivity and help deliver organisational priorities in consistent and equitable ways.
- **Health records** (clinical) are also a key component of corporate documentation and are a vital asset to support delivery of safe and effective care to the CCG's population. Although not a provider of care, the CCG will utilise health records to deliver certain duties and responsibilities (Continuing Healthcare, safeguarding, complaints, for example) and need to manage these in line with relevant requirements of this policy (e.g. held securely).

2. Purpose

2.1. The purpose of this policy is to support the organisation in meeting its obligations in terms of legal and national guidance and to also provide effective governance arrangements for the record management function.

3. Scope

3.1. This policy applies to all CCG employees, including contractors, temporary staff, secondees and honorary employees.

4. Definitions

Item	Definition
Records	Recorded information, in any form, created or received and maintained by the organisation in the transaction of its business or conduct of affairs and kept as evidence of such activity. Examples are provided at **Appendix A.**
Corporate Records	Records that relate to the corporate business of the CCG; examples include (not an exhaustive list): • Corporate governance and assurance activities (e.g. committee minutes, action logs, risk registers, policy framework); • Staffing / personnel activities (e.g. HR); • Health and Safety / Facilities management; • Financial management and accounting; • Commissioning, procurement and contracting activities; • Press / media enquiries.
Electronic Record	An electronic record is an electronic document which has been formally declared as a corporate record. A typical electronic record consists of both electronic content (one or more components) and metadata. While electronic documents can be edited and deleted, electronic records are held in a fixed state, with appropriate access and functional permissions applied.

Item	Definition
Records Management	A discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound. The key components of records management are: • Record creation; • Record keeping; • Record maintenance (including tracking of record movements); • Access and disclosure; • Closure and transfer; • Appraisal; • Archiving; • Destruction.
Records Life Cycle	The life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either destruction, confidential destruction or archival preservation. Records Management policies and procedures form part of the information lifecycle management, together with other processes, such as, a records inventory, secure storage and records audit. **Appendix C** outlines the CCG's Corporate Records Retention and Disposal Schedule.
Folder	A folder is a container for related records. Folders (segmented into parts) are the primary unit of management and may contain one or more records (or markers where applicable).
Naming Convention	A naming convention is a collection of rules which are used to specify the name of a document, record or folder.

Item	Definition
Classification	A systematic identification of business activities (and thereby records) into categories according to logically structured conventions, methods and procedural rules represented in a classification scheme.
Protective Marking	Protective marking is a metadata field applied to an object to show the level of security assigned to an object. A protective marking is selected from a predefined set of possible values which indicate the level of access controls applicable to a folder, record etc. within the file plan hierarchy.
Safe Transfer ('Safe Haven')	Safe Haven is a term used to explain an agreed set of arrangements that are in place in an organisation to ensure person identifiable, confidential and/or sensitive information can be received, stored and communicated safely and securely by FAX. The principles of Safe Haven can be transferred and used when considering the safe transfer of personal confidential data (see the CCG's *Safe Haven Procedure* for further detail).
Disposal	The manner in which a record is disposed of after a period of time. It is the final stage of the record management in which a record is either destroyed or permanently retained.
Users (End Users)	This group comprises those, at all levels of the organisation, who generate and use records in their daily activities. The end user group is a source of much or the material which constitutes the record. Since records systems tends to devolve control to end users at the time of record capture, sound advice and guidance to this group is critical for the maintenance of the quality and accountability.

5. Roles and Responsibilities

Role	Responsibilities
Accountable Officer	The Accountable Officer has overall accountability for records management in the organisation.
Associate Director of Governance	The Associate Director of Governance is responsible for ensuring that appropriate mechanisms are in place to support service delivery and continuity. Records management is integral to this as it will ensure appropriate and accurate information is available as required.
Senior Information Risk Officer (SIRO)	The SIRO is responsible for ensuring that national guidance on the handling and management of information is adhered to. The SIRO is responsible to the Governing Body for ensuring that all information risks are reported and mitigated where possible.
Caldicott Guardian	The organisation's Caldicott Guardian is responsible for ensuring that national guidance on the handling of patient identifiable information is applied across the organisation and is only shared in an appropriate and secure manner.
Head of Corporate Assurance (supported by the Corporate Assurance Team)	The Head of Corporate Assurance is operationally responsible for this policy and is responsible for the overall development and maintenance of the records management system. This role also provides guidance to staff on legal requirements and good practice in relation to records management (e.g. file structures and record naming).
Associate Directors / Senior Managers	The responsibility for local records management is devolved to the relevant Associate Director / Senior Managers within the organisation. Managers have overall responsibility for the management of records generated by their activities, e.g. for ensuring that records controlled within their areas are managed in a way which meets the aims of this policy.
Information Asset Owner (IAO)	A senior member of staff who is the nominated owner for one or more identified information assets of the organisation. It is a core information governance requirement the all Information Assets are identified and that the business importance of those assets is established.

Role	Responsibilities
Information Asset Administrator (IAA)	An operational manager who is familiar with information risks in their business area. Their primary role is to support the IAO to fulfil their responsibilities and ensure that policies and procedures are followed, recognise actual or potential serious incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up-to-date.
All Staff	Under the Public Records Act 1958, all NHS employees are responsible for any records which they create or use in the course of their duties. Therefore, any records created by an employee of the NHS are public records and may be subject to both legal and professional obligations. Individuals must ensure that they keep appropriate records of their work in the CCG and manage those records in keeping with this policy and with any guidance subsequently produced.

6. Record Creation and Classification

6.1 Record creation is one of the most important processes in records management and all staff within the organisation should aim to create good records that can be used in an effective manner.

6.2 It is important that records are kept in context and the best way to achieve this is to 'file' or 'classify' them. Records cannot be tracked or used efficiently if they are not classified or have been classified inappropriately.

6.3 NHS Digital introduced the Government Security Classification Scheme (GSCS) to ensure that the applicable and relevant security controls are set in place in line with the Department for Health, the wider NHS, health and social care and HMG requirements. For further details of the Classification of NHS Information – Marking Guidance, see **Appendix B**.

6.4 Records captured or filed in a corporate filing system must be regarded as authentic or reliable. A common format for the creation of records will ensure that those responsible for record retrieval are able to locate records more easily (e.g. standard naming convention[1] and version control). Where appropriate, documents should be given a review date (e.g. corporate policies).

[1] A naming convention is a common set of rules or guidelines to apply to the naming of electronic records. Staff should give a unique name to each record which is meaningful and reflects the record's content. Naming should be similarly structured where records are linked (e.g. previous versions).

6.5 To ensure quality and continuity of operational services, all records should be kept accurate and up to date. All CCG staff who are responsible for recording information in both paper and electronic format must ensure they fully understand their responsibilities as set out in this policy and remember that records may be used in a court of law.

7. Aims of the CCG's Records Management System

7.1 Records management plays an integral role within the organisation and ensures that the CCG is complying with legislation and best practice, whilst working in a way that ensures that information is stored, used and accessed appropriately.

7.2 The aims of the CCG's Records Management System are to ensure that:

- **The correct records are readily available when needed** – so that staff are able to access information when needed (as appropriate) and that the organisation is able to form a reconstruction of activities or events that have taken place. Records, and the information within them, should be located and displayed in a way consistent with its use, and the current version should be clearly identifiable where multiple versions exist.

- **Records can be interpreted** - the context of the record should be easily understood. It is important that records clearly demonstrate who created or added to the record and when, during which business process, and how the record is related to other records.

- **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.

- **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, despite changes of format.

- **Records are secure** – records are protected from unauthorised or inadvertent alteration or erasure and 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.

- **Records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures which are in line with the requirements of the IGA Records Management Code of Practice for Health and Social Care Act 2016**.**

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

8. Records Maintenance and Storage (Electronic and Hard Copy Records)

8.1. All staff (as defined within the scope of this policy) have a duty for the maintenance and protection of records they use or create.

- Referencing

  Each Directorate should establish and ensure compliance to a document referencing system that meets its business needs and is easily understood by staff members that create, file or retrieve records held in any media. Several types of referencing can be used, e.g. alpha-numeric, alphabetic, numeric or keyword.

  The most common of these is alpha-numeric, as it allows letters to be allocated for a business activity, e.g. HR for Human Resources, followed by a unique number for each electronic record or document created by the HR function. It may be more feasible in some circumstances to give a unique reference to the file or folder in which the records are kept, and identify the record by reference to date and format.

- Naming

  Each Directorate should nominate staff to establish and document file naming conventions in line with national archives advice; i.e.

  - Give a unique name to each record;
  - Give a meaningful name which closely reflects the records content;
  - Express elements of the name in a structured and predictable order;
  - Locate the most specific information at the beginning of the name and the most general at the end; and
  - Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).

- Security Classification

  Emails and documents containing sensitive information (e.g. information that could have damaging consequences is it were lost, stolen or published in the media) should be marked as “Official – Sensitive” (in line with Cabinet Office Government Security Classifications guidance 2018). Such documents include

the CCG incident Response Plans; EPRR Policy or documents relating to the CCG response to a major incident.

- Indexing and Filing

  Each Directorate should establish and document a clear and logical filing structure that aids retrieval of records.

  The register or index is a signpost to where paper corporate records are stored, (e.g. the relevant folder or file), however, it can be used as a guide to the information contained in those records. The register should be arranged in a user friendly structure that aids easy location and retrieval of a folder or file. Folders and files should be given clear logical names that follow the organisation's or directorate's naming convention.

  The filing structure for electronic records should reflect the way in which paper records are filed to ensure consistency. **Filing of corporate records to local drives on PCs and laptops is not appropriate. Files must be saved to the departmental network, to ensure only authorised access is available and that appropriate backups are taken.**

  Likewise, the filing of key organisational paper records or clinical records in desk drawers is not appropriate, departmental accessible secure storage should be used.

- Version Control

  A system of version control must be implemented to enable staff to know that they are working the latest/correct version of the documentation. This may be in the form of a version number and date or by use of document creation date.

8.2. The identification and safeguarding of vital records is necessary for business continuity and will be included as necessary in business continuity plans.

8.3. It is important that the CCG has robust 'tracking and tracing' procedures to provide an audit trail of the movement and location of records. The CCG will maintain an information asset register that clearly identifies business critical information assets (in relation to both electronic and hard copy records) and the safeguards and controls in place to protect them.

8.4. Personal confidential information should only be moved outside NHS premises with explicit approval from the CCG's Caldicott Guardian.

8.5. Records containing person identifiable data or corporate sensitive information must be stored securely in accordance with Data Protection Act 2018.

8.6. The movement and location of paper records should be controlled to ensure that a record can easily be retrieved at any time.

8.7. Final versions of corporate documents will be included on the CCG's local Intranet site to ensure that all staff can have access to the approved versions of policies and corporate documents. This will support compliance with the Freedom of Information Act 2000.

8.8. The records storage areas must comply with health and safety and fire regulations and be considered in accordance with any confidentiality and access issues.

9. Legal and Professional Obligations

9.1 All NHS records are Public Records under the Public Records Act 1958. The organisation will take actions as necessary to comply with the legal and professional obligations as set out in the IGA Records Management Code of Practice for Health and Social Care Act 2016, in particular:

- The Public Records Act 1958;
- The Data Protection Act 2018;
- The Freedom of Information Act 2000;
- Human Rights Act 1998;
- General Data Protection Regulation (GDPR);
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice;
- NHS Digital Data Security and Protection Toolkit;
- Cabinet Office Government Security Classifications guidance 2018;

and any new legislation affecting records management as it arises.

10. Retention and Destruction Schedule

10.1. It is a fundamental requirement that all of the organisation's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the CCG's business functions.

10.2. Keeping unnecessary records uses up valuable space and can incur unnecessary costs. It can also cause problems when trying to retrieve important information, for example, when servicing a request made under the Freedom of Information Act 2000.

10.3. The CCG will adhere to the retention and disposal periods as set out in the Information Governance Alliance (IGA) Records Management Code of Practice for

Health and Social Care Act 2016. **Appendix C** details the retention and disposal schedule for the CCG.

10.4. When a record is deemed to have no further value to the CCG or has reached its assigned retention period, it should then be reviewed and if necessary, destroyed under confidential destruction conditions (as per the disposal actions set out in the IGA Records Management Code of Practice for Health and Social Care Act 2016).

10.5. A local retention and disposal schedule for any records which are not listed in the current version of the IGA Records Management Code of Practice will be agreed by the CCG's Information Governance Steering Group.

10.6. All records which are to be disposed of must be destroyed in a secure manner to ensure the information illegible and irretrievable.

10.7. It can be a criminal offence to destroy information; therefore, the organisation needs to be able to clearly demonstrate that records destruction has occurred appropriately.

10.8. Records that need to be preserved for their archival value should have a clearly documented rationale for keeping beyond their scheduled disposal date. Some records will qualify for archive under the Public Records Act and may be required to be transferred to the local place of deposit. These records should be transferred no later than 20 years from creation.

10.9. The Corporate Assurance Team will hold a central record of documents that have been destroyed under this policy and any records that require keeping beyond their scheduled disposal dates. The record will include the document reference, description and date of destruction.

10.10. Further advice and guidance in relation to any of these points this can be obtained from the Head of Corporate Assurance.

11. Communication, Monitoring and Review

11.1 The CCG will establish effective arrangements for communicating the requirements of this policy and will provide guidance and support to line management in relation to their responsibilities.

11.2 The CCG will annually complete a survey or audit of their records to ensure they understand the extent of their records management responsibilities (Information Flows Mapping and Audit, as required by the Data Security and Protection Toolkit).

11.3 This policy will be reviewed by the author every three years (or sooner if new legislation, codes of practice or national standards are to be introduced), and be

endorsed by the Information Governance Steering Group prior to approval from the Audit and Governance Committee.

11.4 Any individual who has queries regarding the content of this policy, or has difficulty understanding how this policy relates to their role, should contact the policy authors.

12. Staff Training

12.1 All CCG staff will be made aware of their responsibilities for records management and Information Governance through the organisation's induction programme and mandatory training requirements.

13. Equality and Diversity Statement

13.1. The CCG pays due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation, both as a commissioner and as an employer.

13.2. As a commissioning organisation, the CCG is committed to ensuring its activities do not unlawfully discriminate on the grounds of any of the protected characteristics defined by the Equality Act, which are age, disability, gender re-assignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

13.3. The CCG is committed to ensuring that its commissioning activities also consider the disadvantages that some people in our diverse population experience when accessing health services. Such disadvantaged groups include people experiencing economic and social deprivation, carers, refugees and asylum seekers, people who are homeless, workers in stigmatised occupations, people who are geographically isolated, gypsies, roma and travellers.

13.4. As an employer, the CCG is committed to promoting equality of opportunity in recruitment, training and career progression and to valuing and increasing diversity within our workforce.

13.5. To help ensure that these commitments are embedded in the CCG's day-to-day working practices, an Equality Impact Assessment has been completed for, and is attached to, this policy.

14. Interaction with other Policies

14.1 This policy should be read in conjunction with the following CCG documents (where relevant):

- Information Governance Management Framework;
- Policy on the Development and Management of Policy Documents;
- Freedom of Information (FOI) and Environmental Information Regulations (EIR) Policy;
- Information Security Policy;
- Confidentiality and Data Protection Policy.

15. References

Records management Code of Practice for Health & Social Care 2016 - https://digital.nhs.uk/information-governance-alliance

16. Equality Impact Assessment

Date of assessment:	**March 2021**			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Age[2]	No	N/A	N/A	N/A
Disability[3]	No	N/A	N/A	N/A
Gender reassignment[4]	No	N/A	N/A	N/A
Marriage and civil partnership[5]	No	N/A	N/A	N/A
Pregnancy and maternity[6]	No	N/A	N/A	N/A
Race[7]	No	N/A	N/A	N/A

[2] A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).

[3] A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.

[4] The process of transitioning from one gender to another.

[5] Marriage is a union between a man and a woman or between a same-sex couple. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.

[6] Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.

[7] Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.

Date of assessment:	**March 2021**			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Religion or belief[8]	No	N/A	N/A	N/A
Sex[9]	No	N/A	N/A	N/A
Sexual orientation[10]	No	N/A	N/A	N/A
Carers[11]	No	N/A	N/A	N/A

[8] Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.

[9] A man or a woman.

[10] Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none. https://www.equalityhumanrights.com/en/equality-act/protected-characteristics

[11] Individuals within the CCG which may have carer responsibilities.

Appendix A

Examples of Records and Formats
(to be managed in line with the Records Management Code of Practice for Health and Social Care 2016)

Functions:

- Administrative records (including e.g. personnel, incident report forms and risk assessments, estates, financial and accounting records, notes associated with complaint-handling).
- Audio and video tapes, cassettes, CD-ROM.
- Computer databases, output, and disks etc., and all other electronic records.
- Computerised records.
- Data processed for secondary purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes. This can include data for service management, research or supporting commissioning decisions.
- Emails.
- Letter to and from other health professionals (primary or secondary care).
- Material intended for short term or transitory use, including notes and 'spare copies' of documents.
- Microfilm.
- Patient health records of all types (electronic or paper based).
- Photographs, slides or other images.
- Scanned records.
- Tape recordings of telephone conversations.
- Text messages and social media.
- Websites and intranet sites.

(This list is not exhaustive).

Appendix B

Classification of NHS Information – Marking Guidance

NHS CONFIDENTIAL – Appropriate to paper and electronic documents and files containing person-identifiable information, including service users, staff and any other sensitive information.

NHS PROTECT - Discretionary marking that may be used for information classified below NHS Confidential level, but requiring care in handling. Descriptors may also be used as required.

NHS OFFICIAL - Appropriate to paper and electronic documents and files containing sensitive information (e.g. information that could have damaging consequences is it were lost, stolen or published in the media)

Table of descriptors that may be used with 'NHS CONFIDENTIAL' or 'NHS PROTECT' marking	
Category	**Definition**
Appointments	Concerning actual or potential appointments not yet announced.
Barred	Where: (a) there is a statutory (Act of Parliament or European Law) prohibition on disclosure, or (b) disclosure would constitute a contempt of court (information the subject of a court order).
Board (Governing Body)	Documents for consideration by an organisation's Board of Directors, initially in private. *(Note: This category is not appropriate to a document that could be categorised in some other way).*
Commercial	Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs.
Contracts	Concerning tenders under consideration and the terms of tenders accepted.
For Publication	Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date.
Management	Concerning policy and planning affecting the interests of groups of staff. *(Note: Likely to be exempt only in respect of some health and safety issues.)*
Patient Information	Concerning identifiable information about patients.
Personal	Concerning matters personal to the sender and/or recipient.
Policy	Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published).
Proceedings	The information is (or may become) the subject of, or concerned in a legal action or investigation.
Staff	Concerning identifiable information about staff.

Appendix C

Corporate Records Retention and Disposal Schedule

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Audit and Risk			
Audit Reports	6 years	Date of the report	Review, Archive or Destroy under confidential conditions
Risk Registers	10 years	Until superseded	Review, Archive or Destroy under confidential conditions
CCTV			
CCTV images	31 days	Date of images	Review, Archive or Destroy under confidential conditions
Commissioning			
Commissioning decisions (including appeal and decision documentation)	6 years	Date of appeal / decision	Review, Archive or Destroy under confidential conditions
List of approved suppliers	15 years	Date of the latest version	Review, Archive or Destroy under confidential conditions
Tender Documentation (unsuccessful)	6 years	Award of tender	Review, Archive or Destroy under confidential conditions

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Tender Documentation (successful)	6 years	End of contract	Review, Archive or Destroy under confidential conditions
Procurement Documentation, including Business Cases / Clarification Questions / ITQs / Statement of Work / Project Costings	6 years	End of financial year to which the record relates	Review, Archive or Destroy under confidential conditions
Contracts sealed or unsealed	6 years	Termination of contract	Review, Archive or Destroy under confidential conditions
Contracts - financial approval files	15 years	Termination of contract	Review, Archive or Destroy under confidential conditions
Complaints			
Complaints Records (including correspondence, investigation and outcomes)	10 years	Date of file closure	Review, Archive or Destroy under confidential conditions

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Emergency Preparedness, Resilience and Response (EPRR)			
Decision Log, Pocket Log Book, On Call Log Book, Incident-related documents including Debrief Records/Lessons Identified and documents of potential legal interest i.e. major/critical/business continuity/serious incident logs from predecessor organisations, documents presented in court/to coroners, plans, communications, organisational structures and other documents that could fit into this category. Format of records - mixture of paper and electronic.	30 years	Date of last action	Review, Archive or Destroy under confidential conditions
Decision Log, Pocket Book, On Call Log, Log Book, post-exercise reports/Lessons Identified. Format of records - mixture of paper and electronic.	10 years	Date of last action	Review, Archive or Destroy under confidential conditions
Decision Log, Pocket Book, On Call Log, Log Book, on-call-related documents including handover records, reviews/Lessons Identified and documents of potential legal interest i.e. event logs from predecessor organisations, documents presented in court/to coroners, plans, communications, organisational structures and other documents that could fit into this category. Format of records – mixture of paper and electronic.	10 years	Date of last action	Review, Archive or Destroy under confidential conditions
Incident Response Plans, Business Continuity Plans, EPRR Guidance , Standard Operating Procedures, Policy, Strategy, EPRR Core Standards Assurance reviews and reports. Format of records - electronic.	30 years	Date of last action	Review, Archive or Destroy under confidential conditions

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Information Sharing Protocols and Memorandum of Understanding, Mutual Aid Agreements, Service Level Agreements. Format of records -mixture of paper and electronic.	10 years	Date of last action	Review, Archive or Destroy under confidential conditions
Local Health Resilience Partnerships and sub-groups- minutes, papers, action logs, Risk Registers. Format of records - electronic.	30 years	Date of last action	Review, Archive or Destroy under confidential conditions
Ambient voice recording, telephone recording in relation to incident coordination centre. Format of records - electronic.	30 years	Date of last action	Review, Archive or Destroy under confidential conditions
Estates			
Building plans and records of major building work	6 years	Lifetime of the building or disposal of the asset	Review, Archive or Destroy under confidential conditions
Records of minor building work	6 years	Completion of the work	Review, Archive or Destroy under confidential conditions
Finance – Accounting			
Records of financial transactions, including: Invoices Statement Receipts Expense claims Budget forecasting Financial analysis Grant documents for mergers / acquisitions Timesheets	6 years	End of financial year	Review, Archive or Destroy under confidential conditions
Final annual accounts report	20 years	Date of creation	Transfer to place of deposit.

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Finance – Counter Fraud			
Report papers used in the course of a fraud investigation - where fraud is proven	6 years	Completion of legal proceedings	Review, Archive or Destroy under confidential conditions
Report papers used in the course of a fraud investigation - where fraud is not proven	3 years	Completion of investigation / legal proceedings	Review, Archive or Destroy under confidential conditions
Finance – Pay & Pensions			
Records of superannuation paid to staff	10 years	End of financial year	Review, Archive or Destroy under confidential conditions
Records of salaries paid to staff	10 years	End of financial year	Review, Archive or Destroy under confidential conditions
Death Benefit Nomination and Revocation Forms	Keep until employee's 75th birthday	Date of employee leaving	Review, Archive or Destroy under confidential conditions
Personal payroll history, including record of pay, performance pay, overtime pay, allowances, pay enhancements, other taxable allowances, payment for untaken leave, reduced pay, no pay, maternity leave.	Keep until employee's 75th birthday	Date of employee leaving	Review, Archive or Destroy under confidential conditions
Pensions estimates and awards	Keep until employee's 75th birthday	Date of employee leaving	Review, Archive or Destroy under confidential conditions

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Central Employee Payroll Records, including: Full name and date of birth. National Insurance Number. Pensionable pay at leaving. Reckonable service for pension purposes (and actual service where this is different, together with reasons for the difference). Reason for leaving and new employer's name (where known). Amount and destination of any transfer value paid. Amount of any refund of NHS Pension Scheme contributions. Amount and date of any Contributions Equivalent Premium paid. All other papers relating to pensionability not listed above (e.g. papers about pensionability of other employment (including war service); extension of service papers; papers about widower's, widower's, children's and other dependant's pension; correspondence with the Cabinet Office, other departments and pension administrators, or the officer and his/her representatives (MP's, union or others) about pension matters.	Keep until employee's 75th birthday	ate of employee leaving	Review, Archive or Destroy under confidential conditions
Added years	Keep until employee's 75th birthday	Date of employee leaving	Review, Archive or Destroy under confidential conditions
Additional voluntary Contributions (ABC)	Keep until employee's 75th birthday	Date of employee leaving	Review, Archive or Destroy under confidential conditions
Complete sick absence record showing dates and causes of sick leave [as recorded on ESR, does not include copies of sick notes]	Keep until employee's 75th birthday	Date of employee leaving	Review, Archive or Destroy under confidential conditions
Governance			
Annual Publications, including: Annual Plans / Annual Plan reviews / Annual Report and Accounts	20 years	Date of publication / finalisation	Review and consider transfer to a Place of Deposit
Annual Report and Accounts	20 years	Date of publication / finalisation	Review and consider transfer to a Place of Deposit

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Standard Operating Procedures (SOPs)	10 years	Date of publication / finalisation	Review and consider transfer to a Place of Deposit
Policies	10 years	Date of publication / finalisation	Review and consider transfer to a Place of Deposit
Strategies	10 years	Date of publication / finalisation	Review and consider transfer to a Place of Deposit
Published Guidance and Procedures	20 years	Date of publication / finalisation	Review and consider transfer to a Place of Deposit
Merger Pack	10 years	Date of publication / finalisation	Review and consider transfer to a Place of Deposit
Gifts and Hospitality	10 years	Date of gift / hospitality	Review, Archive or Destroy under confidential conditions
General Notification of Interests / Conflicts of Interest Register	6 years	Date last updated	Review, Archive or Destroy under confidential conditions
Annual Reports	20 years	Date of Report	Review and consider transfer to place of deposit.
Performance Reports	10 years	Date of report	Review, Archive or Destroy under confidential conditions
Serious Untoward Incident Reports / Files	20 years	Date of incident	Review, Archive or Destroy under confidential conditions
Meeting Minutes - Executive / Board Level	20 years	Date of meeting	Review and consider transfer to a place of deposit
Meeting Minutes - Below Executive / Board Level	6 years	Date of minutes	Review, Archive or Destroy under confidential conditions
Terms of Reference - Executive / Board Level	20 years	When superseded	Transfer to place of deposit
Terms of Reference - Below Executive / Board Level	6 years	When superseded	Review, Archive or Destroy under confidential conditions

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Health and Safety			
Accident Books (BI 510) and completed Accident Record forms	10 years	Date of last action	Review, Archive or Destroy under confidential conditions
Copies of Reporting of Injuries, Diseases and Dangerous Occurrences Register (RIDDOR) report forms	12 years	Date of accident report	Review, Archive or Destroy under confidential conditions
Equipment Inspection, Reporting & Maintenance Records, including: Completed Ladders and Stepladders inspection forms, Fire alarm and detection system test & maintenance records Inspection and testing of electrical equipment Gas equipment and boiler maintenance records Personal protective equipment issue records Fire evacuation drills, Completed Office H&S Inspection Reports	12 years	Decommission of equipment	Review, Archive or Destroy under confidential conditions
LOLER examination reports for lifts	20 years	Date of report	Review, Archive or Destroy under confidential conditions
Model Risk Assessment (this covers assessments required under several codes of regulations. Each office must have a copy detailing their local arrangements)	10 years	Date of risk assessment	Review, Archive or Destroy under confidential conditions
Fire certificate	20 years	Date of certificate	Review, Archive or Destroy under confidential conditions
Fixed electrical installation inspections	20 years	Date of inspection	Review, Archive or Destroy under confidential conditions
Water Sanitation documentation	10 years	Date of occupation ceases	Review, Archive or Destroy under confidential conditions
Water coolers Sanitation	10 years	Date of sanitation check	Review, Archive or Destroy under confidential conditions

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Completed Risk Assessments for new or Expectant Mothers	6 years	Date of employee leaving	Review, Archive or Destroy under confidential conditions
Completed H&S Audits for Out stationed staff	6 years	Date of employee leaving	Review, Archive or Destroy under confidential conditions
Fire evacuation drills	3 years	Date of fire evacuation drill	Review, Archive or Destroy under confidential conditions
Completed Office H&S Audit Reports	10 years	Date of report	Review, Archive or Destroy under confidential conditions
Human Resources			
Employee / Staff Central Record (includes records for National Directors, Non - Executive Directors, Trust Chairs, Trustees) Including but not limited to contract of employment, changes to terms and conditions, evidence of right to work, security checks and recruitment documentation, job adverts, application forms, job evaluation paperwork, public appointment assessors records, details of work related injuries, details of any exposure to hazardous materials, professional and stat / mandatory training records, details of special and / or unpaid leave periods, e.g. maternity / paternity / adoption leave)	6 years	End of contract of employment	Create staff record summary and transfer all relevant information, then review or destroy main file
Employee / Staff Record - Line Management Records (e.g. sick notes, annual leave records, PDR / appraisal / objective monitoring documentation)	6 years	End of contract of employment	Review, Archive or Destroy under confidential conditions

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Employee / Staff Record - Summary Record Where a summary is made it must contain as a minimum: a summary of the employment history with dates; pension information including eligibility; details of any work related injury; records of any exposure to hazardous materials (including Lead (Control of Lead at Work Regulations 1980), Asbestos (Control of Asbestos at Work Regulations 1996), Compressed Air (Work in Compressed Air Regulations 1996), Radiation (Ionising Radiation Regulations 1985)); professional training history and professional qualifications related to the delivery of care; list of buildings where the member of staff worked and the dates worked in each location	Keep until employee's 75th birthday	End of contract of employment	Review and consider transfer to a place of deposit
Employee / Staff - Occupational Health Reports	Keep until employee's 75th birthday	Date of employee leaving	Review, Archive or Destroy under confidential conditions
Employee / Staff - Occupational Health Report of Staff member under health surveillance	Keep until employee's 75th birthday	Date of employee leaving	Review, Archive or Destroy under confidential conditions
Employee / Staff - Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses	50 years from the date of last entry, or until employee's 75th birthday, **whichever is longer**	Date of employee leaving	Review, Archive or Destroy under confidential conditions
Grievance and / or Disciplinary Case Records	6 years	Closure of investigation	Review, Archive or Destroy under confidential conditions
Employee / Staff Records - Individual Pension Records	Keep until employee's 100th birthday	Date of employee leaving	Review, Archive or Destroy under confidential conditions
Statutory and Mandatory Training Records	10 years	Completion of training	Review, Archive or Destroy under confidential conditions
Training Records (other, not listed elsewhere in this document)	6 years	Completion of training	Review, Archive or Destroy under confidential conditions
Programme evaluation and feedback	6 years	Date of record	Review, Archive or Destroy under confidential conditions

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Applications – unsuccessful	1 year	Notification of unsuccessful application	Review, Archive or Destroy under confidential conditions
ICT			
Disaster recovery plans	6 years	Until superseded	Review, Archive or Destroy under confidential conditions
Documentation relating to computer programmes written in-house	6 years	End of use of programme	Review, Archive or Destroy under confidential conditions
Clinical Protocols These may have preservational value. They may also be routinely captured in clinical governance meetings which may form part of the permanent record (refer to Corporate Governance Records).	25 years	End of use of programme	Review, Archive or Destroy under confidential conditions
IT Equipment Specifications	6 years	Date of specification	Review, Archive or Destroy under confidential conditions
Information Governance			
Data Protection Impact Assessment (DPIA)	6 years	End of processing	Review, Archive or Destroy under confidential conditions
Data Processing Agreement	6 years	End of processing	Review, Archive or Destroy under confidential conditions
Legal			
Litigation dossiers - records/documents relating to any form of litigation / legal advice / legal documents	10 years	Closure of litigation	Review, Archive or Destroy under confidential conditions
Whistle Blowing records	10 years	Closure of investigation	Review, Archive or Destroy under confidential conditions

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Projects / Programmes			
Project / Programme Records, including: Issue and Decision Logs Presentations, Quarterly Reports, Quarterly Reviews Reporting / Reports Planning documents	10 years	Date of completion of the project	Review, Archive or Destroy under confidential conditions
Public / Media / Staff Relations			
Correspondence with branches of the media	7 years	Date of last action	Review, Archive or Destroy under confidential conditions
Reports on media / public relations	7 years	Date of last action	Review, Archive or Destroy under confidential conditions
Press releases	6 years	Date of the press release	Review, Archive or Destroy under confidential conditions
Formal / Statutory / Public Consultations eg. future of the provision of services or National Tariff	6 years	Date of last action	Review, Archive or Destroy under confidential conditions
Internal marketing and communications	3 years	Publication date	Review, Archive or Destroy under confidential conditions
Surveys (patient / staff) - individual responses	Destroy individual survey responses once analysis is complete.	Completion of survey	Review and consider transfer to a place of deposit
Surveys (patient / staff) - analysis	Retain until report completed	Completion of survey	Review and consider transfer to a place of deposit
Surveys (patient / staff)- reports	10 years	Completion of survey	Review and consider transfer to a place of deposit
Public facing website	6 years	When superseded / or at significant change / refresh	Review and consider transfer to a place of deposit
Organisation Intranet	6 years	When superseded / or at significant change / refresh	Review and consider transfer to a place of deposit

Record Description	Recommended Minimum Retention	Trigger Point	Final Action
Information Requests - Freedom of Information / Subject Access Requests / Access to Health Records Requests - requests and responses and any associated correspondence	3 years	Date of disclosure of information	Review, Archive or Destroy under confidential conditions
Information Requests - Freedom of Information / Subject Access Requests / Access to Health Records Requests - where there has been an appeal.	6 years	Date of disclosure of information	Review, Archive or Destroy under confidential conditions
Records Management			
Classification schemes	7 years	Date of classification scheme	Review, Archive or Destroy under confidential conditions
Indexes	7 years	Date of last action	Retain permanently
Disposal schedules	6 years	Date of schedule	Review, Archive or Destroy under confidential conditions
Disposal certificates	7 years	Date of certificate	Review, Archive or Destroy under confidential conditions
Special Events			
Visitors book	3 years	Date of last action	Review, Archive or Destroy under confidential conditions
Event Registration Records	3 years	Date of event	Review, Archive or Destroy under confidential conditions