NHS
Health Education England

Records Management Policy

Version:	2.01
Ratified by:	HEE Executive Team
Date ratified:	26 March 2019
Name and Title of originator/author(s):	Andrew Todd, Information Governance Lead Nicola Wright, Deputy Head of Corporate Affairs
Name of responsible Director:	Lee Whitehead, Director of People & Communications
Date issued:	
Review date:	
Target audience:	All HEE staff creating and maintain records
Document History:	**Version 1** - 7 May 2013: for consideration by Corporate Secretary 15.5.13 Agreed by Lee Whitehead for submission to OMEC **Version 1.1** - IGSG review and update 26/05/2016 **Version 1.2** - IGSG review with additional information 29/07/2016 **Version 1.3** – Ratified by Exec Team December 2017 **Version 2.01** – Draft February 2019

Developing people
for health and
healthcare

www.hee.nhs.uk

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet, and copied to the internet, is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Executive Summary

It is the responsibility of all staff to ensure that they keep appropriate records of their work (either written or in electronic format) and manage those records in keeping with this policy and any other guidance provided by HEE.

Contents

1. Introduction

1.1. Health Education England (HEE) is dependent on its records to operate efficiently and account for its actions. This policy defines a structure for HEE to ensure adequate records are maintained and they are managed and controlled effectively and at best value, commensurate with legal, operational and information needs.

2. Purpose

2.1. HEE's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. They support policy formation and managerial decision making, protecting the interests of HEE and its partners, the rights of its staff and members of the public with whom it has dealings. They support consistency, continuity, efficiency and productivity and help HEE to deliver its services and statutory responsibilities in consistent and equitable ways.

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

2.3. All HEE records are Public Records under the Public Records Acts 1958 and 1967 and must be kept in accordance with the following statutory and NHS guidelines:

- Public Records Acts 1958 and 1967;
- Data Protection Act 2018;
- The General Data Protection Regulation 2016;
- Freedom of Information Act 2000 (section 46);
- Audit Commission, Setting the Record Straight, 1995;
- ISO 15489-1:2016 Information and documentation – Records Management;
- Records Management Code of Practice for Health and Social Care 2016 is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England.

2.4. Failure to comply with the regulations stated in paragraph 2.1 could result in reputational damage to HEE and carries financial penalties of up to 4% of annual turnover or 20 million euros, (whichever is the greater) imposed by the Information Commissioner. This policy applies to all employees and must be strictly observed. Failure to do so could result in disciplinary action.

2.5. Records Management is a core component of business planning and is integrated fully into the annual cycle of business planning.

3. Scope

3.1. This policy relates to all, records held by HEE relating to information created or received in the course of business and captured in readable form in any medium, providing evidence of the functions, activities and transactions of the organisation. They include: -

- Administrative records;
- Records in electronic format; and
- Personal data as defined by the Data Protection Act 2018.

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

3.3. All records created in the course of the business of HEE and corporate records are public records under the terms of the Public Records Acts 1958 and 1967. This includes emails and other electronic records.

4. Duties

4.1. The Chief Executive has overall responsibility for ensuring that records are managed responsibly within HEE.

4.2. The Head of Corporate Affairs and the Information Governance Team are responsible for day to day co-ordination of records management in the organisation, identifying key corporate records and providing guidance and advice on their management and retention.

4.3. The Executive Team will be responsible for ensuring that the policy is implemented across HEE.

4.4. Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) are responsible for ensuring the assets within their services are managed in accordance with this policy, and for maintaining adequate records within the context of legal and regulatory requirements.

4.5. It is the responsibility of all staff to ensure that they keep appropriate records of their work and manage those records in keeping with this policy and with any relevant guidance produced by HEE. Staff should also ensure that they adhere to the retention schedule which can be found in Table 1 of this policy in order to ensure consistency, continuity, efficiency and productivity to help HEE to deliver its services and statutory responsibilities in consistent and equitable ways.

5. Objectives

5.1. There are seven main objectives of this policy:

i) Accountability

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

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

ii) Quality

5.3. Quality – that records are complete and accurate and the information they contain is reliable and their authenticity can be guaranteed.

iii) Accessibility

5.4. Accessibility – that records and the information within them can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held by the organisation.

iv) Security

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

v) Retention and Disposal

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

vi) Training

5.7. Training – that all staff are made aware of their record-keeping responsibilities through training programmes and guidance and where significant new systems are introduced; awareness programmes are put in place to guide staff through the process of change.

vii) Performance Measurement

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

6. Standards to be Maintained

6.1. This policy will be implemented by a series of programmes of work which will deliver clear practice and procedures to include:

i) Records creation (Annex A)

- Creation of adequate records to document essential activities;
- Structured information (content management, version control) to facilitate shared systems based on functional requirements;
- Referencing and information classification for effective retrieval of accurate information;
- Documented guidelines on creation and use of record systems.

ii) Records maintenance (Annex A)

- Assignment of responsibilities to protect records from loss or damage over time;
- Access controls to prevent unauthorised access or alteration of records;
- Defined security levels for access to electronic records and procedures to amend access authorisations as appropriate for new starters and staff leavers;
- Tracking systems to control movement / audit use of records;
- Identification and safeguarding key or vital records;
- Arrangements for business continuity;
- Training and guidance.

iii) Records disposal (Annex A)

- Systematic retention schedules and procedures for consistent and timely disposal;
- Central storage systems for records requiring long-term retention to include electronic archiving systems;
- Mechanisms for regular transfer of records designated for permanent preservation to appropriate archives;
- Secure destruction of confidential information including special category / sensitive personal data.

iv) Training and guidance

- Inclusion of records management functions in job processes where appropriate;
- Generic and specific guidance on record-keeping standards and procedures;
- Training programmes.

v) Performance measurement

- Development of effective indicators and review systems to improve records management standards.

vi) Information classification scheme (Annex A)

- Official – this refers to most of the information that is created or processed by the public sector. (No protective marking is required to be applied to Official information);
- Official-Sensitive – a limited subset of the above which could have more damaging consequences if released inappropriately and may therefore attract additional security measures.

7. Scanning / Digitising Information

7.1 For reasons such as business efficiency and or to address problems with storage space, IAOs and IAAs may consider the option of scanning paper records into electronic format

7.2 Large scale scanning can be a very expensive option and considerations for privacy, availability, access and retention of information should be addressed. Please ensure there is consultation with the Information Governance Team prior to digitising information.

7.3 Staff involved in a process to scan paper records into electronic format with the purpose of discarding the original paper file, should understand the principles of information management encapsulated in Code of Practice BS 10008: 2014 to conform to the provisions of the Records Management Code of Practice.

7.4 By virtue of the Freedom of Information Act 2000, HEE is required to conform to the Code of Practice ‘BS 10008: 2014: Evidential Weight and Legal Admissibility of Electronic Information.

8. Records Security: Work Based and Home Working

8.1 All person identifiable data or commercially sensitive data must be saved securely.

8.2 Staff should not use home email accounts or private computers to hold or store any sensitive records or information which relates to the business activities of HEE.

8.3 Authorised encrypted removable media is permitted to transfer information as per the HEE Information Security Policy, but ideally, person identifiable / sensitive data should not be stored on any removable media, however if there is no alternative ensure this data is deleted once transferred to an identified secure area folder.

8.4 When printing paper records, especially sensitive documents, ensure appropriate measures have been taken and all documents are collected immediately after printing.

8.5 When transferring data either directly or via a third party, ensure security measures and precautions have been actioned by the sender and the receiver.

8.6 Never leave your computer logged on when unattended.

9. Transfer of Records to the National Archive (Public Records Office)

9.1 All records produced by HEE, in any media, are public records and, as such, are subject to the Public Records Acts 1958 and 1967. However, not all public records are worthy of permanent preservation after their administrative usefulness has ended.

9.2 The Information Governance Team will assist, identify and select any notable or precedent cases which are likely warrant permanent preservation in the National Archive.

10. Personal Documents

10.1 It is recognised that staff will occasionally use their work issued computers for their own personal use, which is for material not related to the business of HEE.

10.2 Such material must not be stored on SharePoint, the shared file server on the network or locally on your computers C: drive, as this is not subjected to back up processes and the information could be lost due to computer failure.

11. Equality Impact Assessment (EIA)

11.1 This policy applies to all HEE staff, irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or martial status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership. In implementing the Records Management Policy, HEE will implement reasonable adjustments where appropriate.

12. Education and Training Requirements

12.1 There is an obligation upon every line manager to ensure that staff are informed and instructed with regards to information governance and that such activities are properly recorded, and records maintained.

12.2 As an employee of HEE, you are required to participate in information governance training relevant to you and read this policy document carefully and raise any queries that you may have with your line manager or a member of the Information Governance Team.

13. Monitoring Compliance and Effectiveness

This section identifies how HEE monitors compliance with this policy: -

- Team Managers, Business Managers and the IG Team will periodically monitor and review the handling methods and processes used to manage records effectively in line with this policy;
- Snapshot audits and reviews will be performed on an ad hoc basis; capturing handling processes in real time;
- In the event of non-conformities found within the audits and reviews a report and action plan will be presented to senior management and actions will be considered to mitigate risks;
- Snapshot audits will be presented and discussed at the Information Governance Steering Group (IGSG) and will be presented at senior managers forums within the regional areas;
- Lessons learnt will be discussed at the IGSG and within regional areas.

14. Associated Documentation

- Acceptable Use Policy of Mobile Devices and IT Facilities;
- Freedom of Information Publication Scheme;
- Information Governance Policy;
- Induction;
- Procedure for the creation maintenance and disposal of HEE records (Appendix A);
- Information Security Policy;
- Data Protection Impact Assessment Policy;
- Information Governance and Cyber Security Incident Management Procedure.

15. References

- Public Records Acts 1958 and 1967;
- Data Protection Act 2018;
- General Data Protection Regulation 2016;
- Freedom of Information Act 2000;
- Audit Commission, Setting the Records Straight, 1995;
- ISO 15489-1:2016 Information and documentation – Records Management;
- Records Management Code of Practice for Health and Social Care 2016.

Annex A: Procedure for the creation, maintenance and disposal of HEE records

1. Introduction

1.1 The purpose of this document is to provide Health Education England (HEE) employees with clear procedures for creation, filing and tracking / tracing of electronic and paper corporate records to enable efficient retrieval and effective records management.

2. Scope

2.1 For the purpose of this procedure "records" refer to:

- Corporate and administrative records including personnel, estates, financial and accounting, complaints and trainee records;
- Reports and independent queries;
- Policies and procedures;
- Public involvement and consultation;
- Regular publications and information for the public;
- Communications with the press and media releases.

2.2 It relates to records held in any format, both paper and electronic including emails. It does not relate to medical records.

3. Paper Records vs Electronic Records

3.1 It is recognised that most corporate documents and records held within HEE will be in electronic format. It makes sense not to use up valuable accommodation storing vast amounts of paper.

3.2 Where documents are filed in both electronic and paper format the filing and naming conventions must mirror each other. The procedure described for this process therefore refers to both paper and electronic records.

4. Electronic Storage Areas

4.1 Currently HEE utilises SharePoint and a range of shared drives operating on different systems in order to store most of its electronic records.

4.2 It is recognised that Local Offices each work with their own separate systems and servers. Currently, HEE is developing, utilising and introducing new web-based technologies and systems to enhance collaborative working across the organisation, rationalising HEEs existing system estate to reduce duplication and apply standardisation to information.

4.3 When utilising SharePoint and shared drives the content, purpose and intended audience of the document must be considered, if access to the document is to be limited then the document creator must ensure that the record is in a restricted area.

4.4 The use of unauthorised external web storage or file sharing systems is not permitted unless a Data Protection Impact Assessment (DPIA) is completed. HEE has introduced a web-based technology (SharePoint) to provide a collaboration platform for sharing information across the organisation and externally to our partners.

5. Filing Structure

5.1 Filing structures must be logical to enable the quick and efficient filing and retrieval of records when required and enable implementation of authorised disposal arrangements i.e. archiving, migration to another format or destruction.

5.2 Requests for the creation of departmental folders and security permissions to be set up and modified must come from the Information Asset Owner or Information Asset Administrator within your Directorate or Local Office.

6. Referencing and Name Conventions

6.1 Where a referencing system is used it should be easily understood by staff that create and access electronic or paper documents and records. A simple guide is to think how quickly a new member of staff or a temp could be trained to use the filing system.

6.2 The naming convention should closely reflect the applicable date, record’s content and version. It should also express elements of the name in a structured and predictable order and locate the most specific information at the beginning of the name and the most general at the end.

6.3 At folder level, folder titles must be subject based and where applicable reflect the titles used in corresponding paper filing systems.

6.4 Use of non-specific general titles such as “correspondence” or “miscellaneous” must be avoided. Where a date is required in the title, show this first in YYMMDD format so that documents are listed chronologically.

6.5 Whilst file and folder names should be descriptive, please keep them as short as possible, e.g. use 1 to 4 words maximum when naming folders / up to 25 characters.

6.6 Emails – all the advice and guidance that apply to documents and folders also apply equally to naming emails, but there are other things that should be considered.

6.7 Email titles must accurately describe their content:

- You must change the title of the email if it does not accurately reflect the content;
- You do not need to include ‘email’ as part of the title, as the object icon shows it is an email;
- Save all emails with their attachments;
- Save all emails as Outlook email format (file, save as).

7. Document Version Control

7.1 Some high-level corporate documents such as policies and procedures undergo a consultation process and numerous drafts prior to them being approved. It is therefore necessary that these documents include a Record Reference Sheet, containing metadata describing at what stage they are within this process and which version the document refers to:

Version:	
Ratified by:	
Date ratified:	
Name and Title of originator/author(s):	
Name of responsible Director:	
Date issued:	
Review date:	
Target audience:	
Document History:	

7.2 The document title must contain within it an indication of which version this document is, starting with V0.00. At each redrafting it should be altered to V0.01, V0.02 and so on until it has gone through to the final approval stage at which point it becomes a formal HEE record.

7.3 When the record is next reviewed, for example after a year has elapsed or a major change is required the document version must be renamed V2.00 and then changed to V2.01 and v2.02 and so on as this version goes through the draft approval process.

7.4 ALL information HEE collects, stores, processes, generates or shares to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection.

7.5 EVERYONE who works within HEE (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HEE information or data that they access, irrespective of whether it is protectively marked or not.

8. Filing and Storage of Paper Records

8.1 Paper records and files must be grouped in a logical structure to enable the quick and efficient filing and retrieval of information when required and enable implementation of authorised disposal arrangements, i.e. archiving or destruction.

8.2 HEE is aiming to meet the NHS's target of 2020 to become a paperless organisation. The use of records management and storage facilities should now be limited to historic information.

8.3 Where required, suitable storage areas must be used to ensure records remain accessible and usable through their lifecycle. Access must be controlled through a variety of security measures e.g. authorised access granted to individuals to access storage and filing areas, lockable storage areas**.**

8.4 Records containing personal data should be stored in line with the guidance given in the General Data Protection Regulation 2016 and the Data Protection Act 2018

9. Protective Marking Scheme

9.1 HEE has adopted a new classification scheme for corporate information as it is an expectation from the Department of Health and Social Care (DHSC) for all Arms' Length Bodies (ALBs) to comply. Our approach will satisfy any corporate communications with DHSC, other departments and ALBs.

9.2 In the interim, some NHS organisations may still work to existing IG guidance; consequently, and information received from an NHS organisation may be marked as NHS Confidential which should then be treated as OFFICIAL-SENSITIVE depending on its type.

9.3 The majority of information used by HEE is OFFICIAL. It is highly unlikely HEE will work with SECRET or TOP SECRET information classifications utilised elsewhere within the public sector.

9.4 Two simplified levels of security classifications for information assets within HEE include:

- OFFICIAL – this refers to most of the information that is created or processed by the public sector;
- OFFICIAL-SENSITIVE – a limited subset of the above which could have more damaging consequences if released inappropriately and may therefore attract additional security measures.

9.5 It is very important that, as an author, care is taken in selecting the appropriate protective marking. Over-marking should be avoided, as these risks bringing the system into disrepute as well as introducing inefficiencies such as unnecessarily limiting access increasing the cost of security controls required to protect the information and impairing business efficiency. Equally, under-marking should be avoided which may put the asset at risk of accidental or deliberate compromise through inadequate protection.

9.6 Things to remember about OFFICIAL information:

- Ordinarily OFFICIAL information does NOT need to be marked for non-confidential information;
- A limited subset of OFFICIAL information could have more damaging consequences if it were accessed by individuals by accident or on purpose, lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL classification tier but should have additional measures applied in the form of OFFICIAL-SENSITIVE;
- This marking is necessary for person identifiable information and commercially sensitive information and is applicable to paper and electronic documents / records;
- In addition, to the marking of documents / records as OFFICIAL-SENSITIVE; further detail is required regarding the content of the document or record i.e. OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL-SENSITIIVE: PERSONAL.

OFFICIAL-SENSITIVE: COMMERCIAL

9.7 Definition – commercial information, including that subject to statutory or regulatory obligations, which may be damaging to HEE or a commercial partner if improperly accessed.

9.8 Such documents / records should be marked with caveat OFFICIAL-SENSITIVE: COMMERCIAL or SENSITIVE in capitals at the top and bottom of the page.

OFFICIAL-SENSITIVE: PERSONAL

9.8 Definition – personal information relating to an identifiable individual where inappropriate access could have damaging consequences.

9.9 Such documents / records should be marked with the caveat OFFICIAL-SENSITIVE: PERSONAL.

9.10 In unusual circumstances OFFICIAL-SENSITIVE information may contain both personal and commercial data, in such cases the descriptor OFFICIAL-SENSITIVE will suffice.

10. How to Handle and Store OFFICIAL Information

10.1 EVERYONE is responsible for handling OFFICIAL information with care by:

- Adhering to clear desk policy / procedures;
- Information sharing with the right people;
- Taking extra care when sharing information with external partners i.e. send information to named recipients at known addresses;
- Locking your screen before leaving your computer;
- Using discretion when discussing information out of the office.

11. How to Handle and Store OFFICIAL-SENSITIVE Information

11.1 All OFFICIAL-SENSITIVE material including documents, media and other material should be physically secured to prevent unauthorised access, as a minimum, when not in use.

11.2 At all times OFFICIAL-SENSITIVE: PERSONAL or OFFICIAL-SENSITIVE: COMMERCIAL material should be stored within a secure file network server or within a lockable room, cabinets or drawers.

11.3 Always apply appropriate protection and comply with corporate secure data handling rules:

- Always question whether your information may need stronger protection;
- Make sure documents are not overlooked when working remotely or in public areas, work digitally to minimise the risk of leaving papers on trains etc.;
- Only print sensitive information when necessary;

- Send sensitive information by the secure email route, use password protected documents or use encrypted data transfers;
- The use of an employee's personal email account such as yahoo.co.uk or hotmail.co.uk should not be used for work purposes. Staff should use the work email address provided and apply the security available to safeguard information whilst in transit;
- Encrypt all sensitive information stored on removable media particularly where it is outside the organisation's physical control;
- Store information securely when not in use and use a locked drawer / cabinet if paper is used;
- If faxing the information, make sure the recipient is expecting your fax and double check their fax number prior to sending;
- Take extra care to be discreet when discussing sensitive issues by telephone, especially when in public areas, open plan offices and always try to minimise the use of sensitive details;
- Do not send to internet email addresses e.g. gmail, hotmail etc.;
- Only in exceptional cases, where a business need is identified, should sensitive information be emailed over the internet, in an encrypted format, to the third parties. Contact a member of the Information Governance Team for further advice;
- The use of a pin code or an access card for secure printing is both widely available and preferable way to manage the printing process.

Category	Definition	Marking
Appointments	Concerning actual or potential appointments not yet announced.	OFFICIAL-SENSITIVE: COMMERCIAL
Barred	Where there is a statutory (Act of Parliament or European Law) prohibition or disclosure, or disclosure would constitute a contempt of Court (information subject to a court order)	OFFICIAL-SENSITIVE: COMMERCIAL
Board	Documents for consideration by an organisation's Board of Directors, initially, in private (Note: this category is not appropriate to a document that would be categorised in some other way)	OFFICIAL-SENSITIVE: COMMERCIAL
Commercial	Where disclosure would be likely to damage a commercial undertaking's (third party) processes or affairs	OFFICIAL-SENSITIVE: COMMERCIAL
Contracts	Concerning tenders under consideration and the terms of tenders accepted	OFFICIAL-SENSITIVE: COMMERCIAL
For publication	Where it is planned that the information in the completed document will be published at a future date (even if not yet determined)	
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)	OFFICIAL-SENSITIVE: COMMERCIAL

Service user information	Concerning identifiable information about service users (our trainees)	OFFICIAL-SENSITIVE: PERSONAL
Personal	Concerning matters personal to the sender and / or recipient	OFFICIAL-SENSITIVE: PERSONAL
Policy	Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published).	OFFICIAL-SENSITIVE: COMMERCIAL
Proceedings	The information is (or may become) the subject of or concerned in a legal action or investigation.	OFFICIAL-SENSITIVE: COMMERCIAL
Staff	Concerning identifiable information about staff	OFFICIAL-SENSITIVE: PERSONAL

12. Retention and Destruction

12.1 It is good practice to review on a regular basis information which is held in individual file directories and filing systems. Files should be retained in line with the minimum retention periods as specified in the Records Management Code of Practice for Health and Social Care 2016. An extract covering information relevant to HEE is included within Table 1 below.

12.2 Table 1 provides a non-exhaustive summary of the minimum retention period for each type of non-health record. Records, whatever the media, may be retained for longer than the minimum period.

12.3 However, records should not ordinarily be retained for more than 20 years. The National Archives should be consulted where a longer period that 20 years is required. HEE should also remember that records containing personal information are subject to the General Data Protection Regulation 2016 and the Data Protection Act 2018.

Table 1 - Summary: Business and Corporate Non-Health Records Retention Schedule

Record type	Retention start	Retention period	Action at end of retention period	Notes
Corporate Governance				
Accident forms	Date of accident	10 years	Review and if no longer need confidentially destroy	
Accident register	Date of accident	10 years	Review and if no longer need confidentially destroy	RIDDOR - Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
Annual / Corporate Reports	Creation	3 years	Review and if no longer needed destroy	
Audit Records (e.g. organisational audits, records audits, systems audits)	Completion of audit	2 years	Review and if no longer need confidentially destroy	Internal and external in any format

Record type	Retention start	Retention period	Action at end of retention period	Notes
Board meetings	Creation	Before 20 years but as soon as practicably possible	Review and if no longer needed destroy	
Board meetings (closed boards)	Creation	May retain for 20 years	Review and if no longer needed confidentially destroy	
Chief Executive Records	Creation	May retain for 20 years	Review and if no longer needed confidentially destroy	
Committees listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practicably possible	Review and if no longer needed confidentially destroy	
Committees / Groups / Sub-Committees not listed in the scheme of delegation	Creation	6 years	Review and if no longer needed confidentially destroy	Includes minor meetings / projects and departmental business meetings

Record type	Retention start	Retention period	Action at end of retention period	Notes
Destruction certificates or electronic metadata destruction stub or record of information destroyed held on physical media	Destruction of record or information	20 years	Review and if no longer needed confidentially destroy	Records documenting the archiving, transfer to public records archive or destruction or records
Diaries (office)	End of year to which the diary relates	1 year	Review and if no longer needed confidentially destroy	
Health and Safety documentation	From creation	3 years	Review and if no longer needed confidentially destroy	
History of organisation or predecessors, its organisation and procedures (e.g. establishment order)	From organisation end	20 years	Review and if no longer needed destroy	
Incidents (serious)	Date of incident	20 years	Review and if no longer needed confidentially destroy	

Record type	Retention start	Retention period	Action at end of retention period	Notes
Incidents (not serious)	Date of incident	10 years	Review and if no longer needed confidentially destroy	
Indices (records management)	Creation	20 years	Review and if no longer needed destroy	Registry lists of public records marked for permanent preservation, or containing the record or management of public records
	Creation	20 years	Review and if no longer needed confidentially destroy	File lists and document lists where public records or their management are not covered
Non-clinical quality assurance records	End of year to which the assurance relates	12 years	Review and if no longer needed confidentially destroy	
Policies, strategies and operating procedures including business plans	Creation	Life of organisation plus 6 years	Review and if no longer needed confidentially destroy	Administrative and strategy documents including local delivery plans Policy documents may have archival value
Receipts for registered and recorded mail	End of financial year	2 years	Review and if no longer needed confidentially destroy	

Record type	Retention start	Retention period	Action at end of retention period	Notes
Reports (major)	Creation	20 years	Review and if no longer needed confidentially destroy	
Requisitions	Creation	10 months	Review and if no longer needed confidentially destroy	
Communications				
Intranet site	Creation	6 years	Review and if no longer needed confidentially destroy	
Press releases and important internal communications	Release date	7 years	Review and if no longer needed destroy	
Public consultations	End of consultation	5 years	Review and if no longer needed confidentially destroy	
Website	Creation	6 years	Review and if no longer needed destroy	

Record type	Retention start	Retention period	Action at end of retention period	Notes
Staff Records and Occupational Health Although pension information is routinely retained until 100th birthday by the NHS Pensions Agency employers must retain a portion of the staff record until the 75th birthday				
Job advertisements	Closure of advertisement	1 year	Review and if no longer needed destroy	
Job applications (successful)	On termination of employment	3 years	Review and if no longer needed confidentially destroy	
Job applications (unsuccessful)	From date of interview	1 year	Review and if no longer needed confidentially destroy	
Job descriptions	From being revised, superseded or obsolete.	3 years	Review and if no longer needed confidentially destroy	
Letters of appointment	After employment has ended or until 75th birthday whichever is later	6 years	Review and if no longer needed confidentially destroy	

Record type	Retention start	Retention period	Action at end of retention period	Notes
Occupational health reports	Staff member leaves	Keep until 75th birthday	Review and if no longer needed confidentially destroy	
Occupational health report of staff member under health surveillance	Staff member leaves	Keep until 75th birthday	Review and if no longer needed confidentially destroy	
Pension forms	Staff member leaves	7 years	Review and if no longer needed confidentially destroy	HMRC Technical Pensions Notes for registered pension schemes under regulation 18 of SI2006/567- 'RPSM12300020' Scheme Administrator Information Requirements and Administration for General Retention of Records
Staff record	Staff member leaves	Keep until 75th birthday (see notes)	Review and if no longer needed confidentially destroy	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. May be destroyed 6 years after the staff member leaves or the 75th birthday, whichever is sooner, if a summary has been made. The 6-year retention period is to consider any ET claims or EL claims that may arise after the employee leaves NHS employment, requests for information from the NHS pensions agency etc.
Staff Record Summary	6 years after the staff member leaves	75th Birthday	Review and if no longer needed confidentially destroy	

Record type	Retention start	Retention period	Action at end of retention period	Notes
Timesheets (original record)	Creation	2 years	Review and if no longer needed confidentially destroy	Timesheets (original record)
Staff training records	Creation	See Notes	Review and if no longer needed confidentially destroy	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role The IGA recommends: **Clinical training records** - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer **Statutory and mandatory training records -** to be kept for ten years after training completed **Other training records -** keep for six years after training completed
Procurement				
Contracts sealed or unsealed	End of contract	6 years	Review and if no longer needed confidentially destroy	Limitation Act 1980
Contracts – financial approval files	End of contract	15 years	Review and if no longer needed confidentially destroy	

Record type	Retention start	Retention period	Action at end of retention period	Notes
Contracts – financial approved suppliers' documentation	When supplier finishes work	11 years	Review and if no longer needed confidentially destroy	Consumer Protection Act 1987
Delivery notes	Close of financial year	2 years	Review and if no longer needed confidentially destroy	
Tenders (successful)	End of contract	6 years	Review and if no longer needed confidentially destroy	Limitation Act 1980
Tenders (unsuccessful)	Award of tender	6 years	Review and if no longer needed confidentially destroy	Limitation Act 1980
Estates				
CCTV (where HEE owned)		See ICO Code of Practice	Review and if no longer needed confidentially destroy	ICO Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf The length of retention must be determined by the purpose for which the CCTV has been deployed. The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft)

Record type	Retention start	Retention period	Action at end of retention period	Notes
Equipment monitoring and testing and maintenance work	Completion of monitoring or test	10 years	Review and if no longer needed confidentially destroy	
Leases	Termination of lease	12 years	Review and if no longer needed confidentially destroy	The grant of leases, licences and other rights over property
Other items relating to Estates will not generally be held by HEE but by the landlord of each building occupied				
Finance				
Accounts	Close of financial year	3 years	Review and if no longer needed confidentially destroy	Includes all associated documentation and records for the purpose of audit as agreed by auditors
Advice notes (payment)	Receipt of advice note	18 months	Review and if no longer needed confidentially destroy	
Audit records (internal and external audit) – original documents	Completion of audit	2 years	Review and if no longer needed confidentially destroy	

Record type	Retention start	Retention period	Action at end of retention period	Notes
Audit reports (internal and external audit) – including management letters, value for money reports and system / financial accounts	Formal completion by statutory auditor	2 years	Review and if no longer needed confidentially destroy	
Bank statements	Completion of audit	2 years	Review and if no longer needed confidentially destroy	
BACS records	End of financial year	6 years	Review and if no longer needed confidentially destroy	
Benefactions	End of financial year	8 years	Review and if no longer needed confidentially destroy	These may already be in the financial accounts and may be captured in other records/reports or committee papers
Budgets	Completion of audit	2 years	Review and if no longer needed confidentially destroy	Including working papers, reports, virements and journals

Record type	Retention start	Retention period	Action at end of retention period	Notes
Creditor payments	End of financial year	3 years	Review and if no longer needed confidentially destroy	
Debtor records cleared	Close of financial year	2 years	Review and if no longer needed confidentially destroy	
Debtor records not cleared	Close of financial year	6 years	Review and if no longer needed confidentially destroy	
Donations	Close of financial year	6 years	Review and if no longer needed confidentially destroy	
Staff expenses (including travel and subsistence claims and authorisation)	Close of financial year	6 years	Review and if no longer needed confidentially destroy	
Final annual accounts report (one set only)	Creation	Before 20 years	Review and if no longer needed confidentially destroy	

Record type	Retention start	Retention period	Action at end of retention period	Notes
Financial records of transactions	End of financial year	6 Years	Review and if no longer needed confidentially destroy	Invoices and ledgers Limitation Act 1980
Funding data	End of financial year	6 years	Review and if no longer needed confidentially destroy	
PAYE records	Termination of employment	6 years	Review and if no longer needed confidentially destroy	
Payments	End of financial year	6 years	Review and if no longer needed confidentially destroy	
Petty cash	End of financial year	2 Years	Review and if no longer needed confidentially destroy	
Private Finance initiative (PFI) files	End of PFI	Lifetime of PFI	Review and if no longer needed confidentially destroy	

Record type	Retention start	Retention period	Action at end of retention period	Notes
Salaries paid to staff	Close of financial year	10 years after termination of employment	Review and if no longer needed confidentially destroy	For superannuation purposes, organisations may wish to retain such records until the subject reaches benefit age
Superannuation records (accounts and registers)	Close of financial year	10 years	Review and if no longer needed confidentially destroy	
Tax forms	Close of financial year	6 years	Review and if no longer needed confidentially destroy	
Project and Programme Management Records including Business Cases (refer to notes and definitions)				
Project files (RPA high risk and over £50m) completed projects only	Project completion	25 years for second review	Review and if no longer needed confidentially destroy	
Project files (Organisational Portfolio or RPA medium risk and over £100k) completed projects only	Project completion	10 years	Review and if no longer needed confidentially destroy	Organisational Portfolio Office Archive

Record type	Retention start	Retention period	Action at end of retention period	Notes
Project files (Local and RPA low risk and under £100k) on completion, including abandoned or deferred projects of any risk level	Project end	5 years	Review and if no longer needed confidentially destroy	Local documents archive
Project team files (summary retained)	Project end	2 years	Review and if no longer needed confidentially destroy	Local / national team documents archive
Legal, Complaints and Information Rights				
Complaints case file	Closure of incident (see notes)	10 years	Review and if no longer needed confidentially destroy	http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf The incident is not closed until all subsequent processes have ceased including litigation.
Documentation relating to computer programmes written in-house	End of software lifetime	Lifetime of software	Review and if no longer needed confidentially destroy	
Fraud case files / investigations	Closure of case	6 years	Review and if no longer needed confidentially destroy	

Record type	Retention start	Retention period	Action at end of retention period	Notes
Freedom of Information (FOI) requests and responses and any associated correspondence	Closure of FOI request	3 years	Review and if no longer needed confidentially destroy	Freedom of Information Act 2000 Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical to keep a summary of the redactions.
FOI requests where there has been a subsequent appeal	Closure of appeal	6 years	Review and if no longer needed confidentially destroy	Freedom of Information Act 2000
Industrial relations (not routine staff matters) including tribunal case records	Close of financial year	10 years	Review and if no longer needed confidentially destroy	Some organisations may record these as part of the staff record but, in most cases, they will form a distinct separate record either held by the staff member/manager or by the payroll team for processing.
Litigation records	Closure of case	10 years	Review and if no longer needed confidentially destroy	Where legal action has commenced keep as advised by legal representatives
Parliamentary Questions (PQs) and MP enquiries	Closure of request	10 years	Review and if no longer needed confidentially destroy	As these documents include all information provided by HEE in response to a PQ (e.g. background or the Minister may amend the response) all of which may not be used in the response and therefore will not be in the public domain of the House of Commons records

Record type	Retention start	Retention period	Action at end of retention period	Notes
Patents / trademarks / copyright / intellectual property (copyright declaration forms)	End of lifetime of patent or termination of licence/ action	Lifetime of patent or 6 years from end of licence/ action	Review and if no longer needed confidentially destroy	Copyright, Designs & Patents Act 1998
Requests for access to records other than FOI or Subject Access Requests	Closure of request	6 years	Review and if no longer needed confidentially destroy	
Software licences	End of lifetime of software	Lifetime of software	Review and if no longer needed confidentially destroy	
Subject Access Request (SAR) and disclosure correspondence	Closure of SAR	3 years	Review and if no longer needed confidentially destroy	General Data Protection Regulation 2016 Data Protection Act 2018
Subject Access Request where there has been a subsequent appeal	Closure of appeal	6 years	Review and if no longer needed confidentially destroy	General Data Protection Regulation 2016 Data Protection Act 2018

Record type	Retention start	Retention period	Action at end of retention period	Notes
Workforce				
Electronic or hard copy trainee file (includes NTN holders, core trainees and LATs)	CCT date or date of having left training	TBC	Review and if no longer needed confidentially destroy	**Please note:** The trainee record retention policy is currently under review and requires a national decision regarding an appropriate retention period.
Workforce administration records	End of process	TBC	Review and if no longer needed confidentially destroy	Matching process data LAU representative ARCP notes **Please note:** The trainee record retention policy is currently under review and requires a national decision regarding an appropriate retention period.
	Creation / initial use	TBC	Review and if no longer needed confidentially destroy	Rotation grids ARCP invites ARCP timetables / lay representative log Any other workforce file containing personal data stored electronically **Please note:** The trainee record retention policy is currently under review and requires a national decision regarding an appropriate retention period.
	CCT date or date of having left training	TBC	Review and if no longer needed confidentially destroy	Official correspondence relating to a specific trainee sent by the relevant college, trainers or other body **Please note:** The trainee record retention policy is currently under review and requires a national decision regarding an appropriate retention period.

Record type	Retention start	Retention period	Action at end of retention period	Notes
Electronic and hard copy LTFT training records	CCT date or date of having left training	TBC	Review and if no longer needed confidentially destroy	Eligibility forms Approval forms Log of LTFT records **Please note:** The trainee record retention policy is currently under review and requires a national decision regarding an appropriate retention period.
Recruitment				
Electronic and hard copy interview documentation (including academic sub-speciality, speciality and dental recruitment)	Date of interview	1 year	Review and if no longer needed confidentially destroy	Interview score sheets Unsuccessful candidate packs containing interview documents Lat chair notes Any other paperwork containing candidate identifiable material
IDT records	Completion of IDT	1 year	Review and if no longer needed confidentially destroy	Application forms submitted via the application portal Supporting documents submitted via the application portal and email Transfer packs containing trainee documentation Email enquiries submitted to the national IDT mailbox Log of transfer containing personal data
Applicant enquiries	Enquiry / phone call received	1 year	Review and if no longer needed confidentially destroy	Enquiries submitted via the applicant enquiries online portal Log of enquiries submitted via the applicant enquiries online portal Log of phone calls received via the applicant enquiries phone service

Record type	Retention start	Retention period	Action at end of retention period	Notes
Confidential enquiries	Enquiry received	1 year	Review and if no longer needed confidentially destroy	Submissions and accompanying supporting evidence made to the confidential enquiries' mailbox Any associated correspondence saved electronically or s hard copy, including any tracing logs containing personal data
Fitness to practice declarations	Declaration	1 year	Review and if no longer needed confidentially destroy	Submissions and accompanying supporting evidence made to the fitness to practice mailbox Any associated correspondence saved electronically or hard copy, including any tracking logs containing personal data
Case Management				
Electronic and hard copy relocation records (stored within training files)	CCT date or date of having left training	6 years	Review and if no longer needed confidentially destroy	Eligibility forms Relocation claim forms Excess travel claim forms Log of relocation payments
Trainee in difficulty records	CCT date or date of having left training	TBC	Review and if no longer needed confidentially destroy	Electronic confidential file Electronic timeline and action log GMC letters and official correspondence **Please note:** The trainee record retention policy is currently under review and requires a national decision regarding an appropriate retention period
Miscellaneous				
Non-staff expense claims log and claim forms	Receipt of expense form	TBC	Review and if no longer needed confidentially destroy	Logs relating to lay chair / panel member / candidate / trainees expense claims and forms **Please note:** The trainee record retention policy is currently under review and requires a national decision regarding an appropriate retention period

Record type	Retention start	Retention period	Action at end of retention period	Notes
National or Centralised				
Sponsorship records		1 year	Review and if no longer needed confidentially destroy	Tier 2 correspondence, identity documents, sponsorship details and tracking logs saved electronically, in sponsorship email folders or hard copy
	End of the migrant's sponsorship **or** if the migrant is no longer sponsored, the point at which a Home Office Compliance Officer has examined and approved the documents; whichever is the shorter period	1 year	Review and if no longer needed confidentially destroy	Tier 4 correspondence, identity documents, sponsorship details and tracking logs saved electronically, in sponsorship email folders or hard copy
	Sponsorship end	1 year	Review and if no longer needed confidentially destroy	Tier 5 and GMC sponsorship correspondence, identity documents, sponsorship details and tracking logs saved electronically, in sponsorship email folders or hard copy