Corporate Document and Records Management Policy

NHS England

Corporate Document and Records Management Policy

Version number: 4.0

First published: April 2013

Date updated: June 2022

Next review date: November 2023

Policy prepared by: E Ward/L Ince/L Gollick

Policy Owner: C Mitchell

Brief summary of changes since previous version:

Version 3.0

- Records Management Glossary of Abbreviations and Acronyms removed as appendix and reference added in Section 5.5 to the live Acronym Register
- Appendix B updated in line with current naming convention and version control guidance.
- 1.4 Instant Messages added as a record type
- 2.1 Inquiries Act added
- 5.7.2 Reference to the Primary Care Retention Schedule added
- 5.8.6 Added to reflect the role of the new NHSEI Inquiry Hub
- 5.9.7 Updated to reflect the role of the Collaboration Drives
- 9.13 Added to reflect the use of instant messaging
- Roles updated throughout to reflect the role of the Senior Lead – Corporate Records Management

Version 4.0

- Removal of NHS Improvement and update of logo

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet 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.

Contents

1. Purpose

1.1 All NHS England staff members must ensure they are familiar with the contents of this joint policy, which describes the standards of practice we require in the management of our corporate records. It is based on current legal requirements and professional best practice.

1.2. All organisations need to keep records of its activities, patients and the public would rightly expect that NHS England maintains records on its activities and decisions that affect their health service in an exemplary way.

1.3. Records and Documents are different. Documents consist of information or data that can be structured or unstructured and accessed by people in NHS England. Records provide evidence of the activities of functions and policies. Records have strict compliance requirements regarding their retention, access and destruction, and generally have to be kept unchanged. Conversely, all records are documents.

1.4. This policy relates to all documents and records held by NHS England, regardless of format, including, but not limited to, email, paper, digital, instant messages, social media, videos and telephone messages.

1.5. Records are created to provide information about what happened, what was decided, and how to do things. Individuals cannot be expected or relied upon to remember or report on past policies, discussions, actions and decisions accurately all of the time. So, as part of their daily work they keep a record – by updating a register or database, writing a note of a meeting or telephone call, audio recordings of customer interaction or filing a letter or email – which ensures that they and their successors have something to refer to in the future.

1.6. Records are a valuable resource because of the information they contain. High-quality information underpins the delivery of high-quality evidence-based healthcare. Information has most value when it is accurate, up-to-date and accessible when it is needed. An effective records management function ensures that information is properly managed and is available whenever and wherever there is a justified need for that information, and in whatever media it is required.

1.7. Records management is about controlling records within a framework made up of policies, standard operating procedures, systems, processes and behaviours. Together they ensure that reliable evidence of actions and decisions is kept and remains available for reference and use when needed, and that the organisation benefits from effective management of one of its key assets, its records.

1.8. A records retention schedule is a control document. It sets out the classes of records which NHS England retains and the length of time these are retained before a final disposition action is taken (i.e. destruction or transfer to a permanent place of deposit, such as The National Archives. It applies to information regardless of its format or the media in which it is created or might be held. All staff members should be familiar with this records retention schedule and apply retention periods to records.

1.9. A records management policy is a cornerstone of effective management of records in an organisation. It will help to ensure NHS England keeps the records they need for business, regulatory, legal and accountability purposes.

1.10. The purpose of this policy is to establish a framework in which NHS England records can be managed, and to provide staff members with a high-level overview of the legal obligations that apply to NHS records.

1.11. Documents will need to be declared as a record before records management procedures and policies are applied to them. To declare a document as a record at NHS England, it must be stored and declared in the collaboration drive environment.

2. Background

2.1. NHS England will take action as necessary to comply with the legal and professional obligations set out for records, and in particular:

- Public Records Act 1958
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Inquiries Act 2005
- Access to Health Records Act 1990
- Regulation of Investigatory Powers Act 2000
- NHS Records Management Code of Practice 2021
- NHS Information Governance: Guidance on Legal and Professional Obligations
- UK General Data Protection Regulation 2021 (GDPR)

a. The Public Records Act 1958 is an Act of Parliament to make new provision with respect to public records and the Public Record Office, and for connected purposes. It includes duties about selection and preservation of public records, places of deposit, access and destruction.

b. The Data Protection Act 2018 is an Act of Parliament which regulates the processing of personal data relating to living individuals, including the obtaining, holding, use or disclosure of such information. Access to the health records of living patients is governed by this Act

c. The Freedom of Information Act 2000 is an Act of Parliament that makes provision for the disclosure of information held by public authorities or by persons providing services for them. The Lord Chancellor's Code of Practice on the management of records is issued under section 46 of this Act.

d. The Inquiries Act 2005 is an Act of the Parliament of the United Kingdom. Public inquiries investigate issues of serious public concern, scrutinising past decisions and events and can request disclosure of documents and records as evidence. Public inquiries are conducted on behalf of the Crown, which therefore means that records created or given to the inquiry are public records as defined by the Public Records Act 1958.

e. The Access to Health Records Act 1990 is an Act of Parliament that regulates access to the health records of a deceased person.

f. The Regulation of Investigatory Powers Act 2000 which permit the 'interception' of communications. Such interception must be proportionate to the needs of the organisation, society and the users of the communication system.

g. The NHS Records Management Code of Practice 2021 was published NHSX in 2021. It is a best practice guide for the management of records for those who work within or under contract to NHS organisations in England. They are based on legal requirements and professional best practice.

h. NHS Information Governance: Guidance on Legal and Professional Obligations provides guidance on the range of legal and professional obligations that affect the management, use and disclosure of information.

i. The UK GDPR is the UK General Data Protection Regulation. It is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

2.2. Failure to comply with the GDPR or DPA could result in reputational damage to NHS England and carries financial penalties of up to £17 million, or 4% of turnover imposed by the Information Commissioner. Furthermore, individuals can be prosecuted for knowingly or recklessly disclosing, procuring, or obtaining personal data. This policy applies to all employees and must be strictly observed. Failure to do so could result in disciplinary action.

3. Scope

3.1. All NHS England directorates fall within the scope of this document. This includes staff who are employed on a permanent or fixed term basis, contractors, temporary staff and secondees.

3.2. Moreover, staff of the following NHS areas are also within the scope of this document:

- All Commissioning Support Units
- Strategic Clinical Networks
- Clinical Senates
- Offices (e.g. Chairs, Professional Committees)
- Sustainability and Transformation Partnerships
- NHSX
- All other NHS England hosted bodies.

4. Roles and Responsibilities

4.1. The Chief Executive, through the Executive Management Team is accountable for Records Management for NHS England records.

4.2. The National Director of Transformation and Corporate Operations Directorate has the lead responsibility for Records Management and for ensuring this policy is implemented and becomes an active document within NHS England.

4.3. The Data Protection Officer has responsibility for informing, advising and monitoring compliance with data protection principles in relation to this procedure.

4.4. The Senior Lead – Corporate Records Management has operational responsibility for the Records Management Policy and is responsible for the overall development and maintenance of the Records Management Framework and for ensuring this policy complies with legal and regulatory edicts. They are also responsible for providing learning and development with key learning points from this policy and for monitoring compliance with the policy to assess its overall effectiveness.

4.5. The Senior Lead – Corporate Records Management is responsible for developing and supporting a culture of high-quality records management practice across NHS England and to deliver associated organisational benefits. They are also responsible for knowing what records NHS England holds and where they are, by conducting regular audits of records working closely with the IG Assurance team

4.6. The Senior Lead – Corporate Records Management is responsible for ensuring that records created by NHS England are stored securely and that access to them is controlled.

4.7. The Director of HR for both NHS England, is responsible for the application of this policy in respect of ensuring effective NHS England employee records management and for managing access requests for those records made under the Data Protection Act 2018.

4.8. Information Asset Owners are responsible for ensuring the asset they 'own' is managed in accordance with this policy, and also for maintaining adequate records within the context, both legal and regulatory, of the business area the asset operates. For example, at NHS England, Estates and Facilities must be able to demonstrate how they comply with current Health and Safety legislation.

4.9. Information Asset Administrators if appointed for an asset, are responsible for assisting the Information Asset Owners in the management of the records that they 'own', in accordance with point 4.8

4.10. Records and Information Management Coordinators within each business area will champion records and information management from a local level supporting their team in records management matters and ensuring good records management within their area. Roles and responsibilities are outlined in Appendix A.

4.11. All staff are responsible for keeping a record of any significant business transaction conducted as part of their duties for NHS England. The record should be saved appropriately, a retention period assigned, and access controls applied if necessary.

5. Corporate Level Procedures

5.1. This policy covers the management of both documents and records in NHS England. The policy sets in place the strategic governance arrangements for all documents and records produced and received by NHS England in accordance with agreed best practice as well as the principles established in ISO 15489 (the International British Standard for Records Management).

5.2. This policy is mandatory and applies to all information in all formats. It covers all stages within the information lifecycle, including create/receive, maintain/use, document appraisal, declare as a record, record appraisal, retention and disposition.

5.3. Staff members must not alter, deface, block, erase, destroy or conceal records with the intention of preventing disclosure under a request relating to the Freedom of Information Act 2000 or the Data Protection Act 2018.

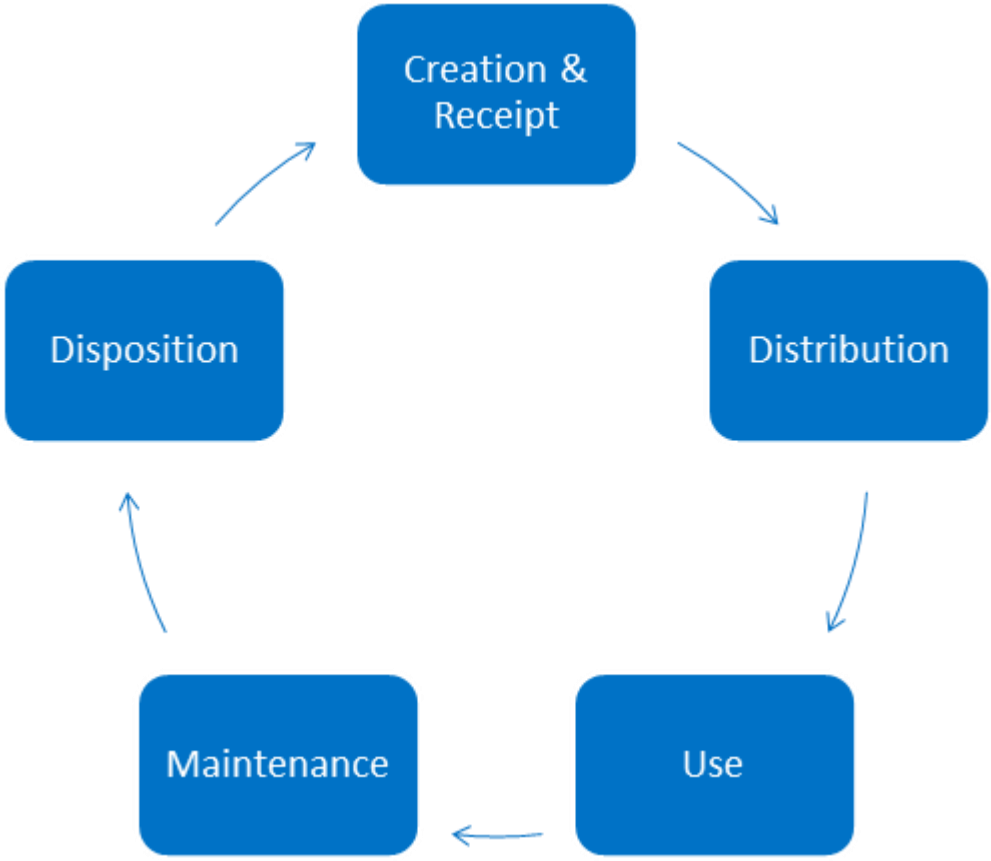
5.4. Staff members are expected to manage records about individuals in accordance with this policy irrespective of their race, disability, gender, age, sexual orientation, religion or belief, or socio-economic status.

5.5. Where records contain any abbreviations or acronyms which are not listed in the Records Management Glossary of Abbreviations and Acronyms please contact the Records Management team to ensure your abbreviation is added to the organisation's Acronym Register.

6. Records and Information Life Cycle Management

6.1. Records and Information Management plays an integral role within NHS England and as it underpins effective information sharing within our organisation and externally to patients and suppliers. The law requires certain records to be kept for a defined retention period; however records are used on a daily basis for internal purposes to help make decisions, provide evidence,

etc. Using the diagram overleaf, you can learn more about each of the 5 steps in the Records Life Cycle.



- Stage 1: Creation and Receipt

  This part of the life cycle is when we put pen to paper, make an entry into a database or start a new electronic document. It is known as the first phase. It can be created by internal employees or received from an external source and it is complete and accurate.

- Stage 2: Distribution

  Distribution is managing the information once it is created or received whether it is internal or external. It occurs when records are sent to someone for which they were intended or were copied. Records are distributed when photocopied, printed, attached to an email, hand delivered or regular mail, etc. After records are distributed, they are used.

- Stage 3: Use

This stage takes place after information is distributed. This is when records are used on a day to day basis to help generate organisational decisions, document further action or support other NHS England operations. It is also considered the Active Phase.

- Stage 4: Maintenance

Maintenance is when records are not used on a day to day basis and are stored in the Records Management system. Even though they are not used on a day to day basis, they will be kept for legal or financial reasons until they have met their retention period. The maintenance phase includes filing, transfers and

retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business decision. Records should not be removed from a Records Management system; the information should be copied and tracked to ensure no amendments were made.

- Stage 5: Disposition

Disposition is when a record is less frequently accessed, has no more value to NHS England or has met its assigned retention period. It is then reviewed and if necessary, destroyed under confidential destruction conditions. Not all records will be destroyed once the retention period has been met. Any records that have historical value to NHS England will be retained for 20 years and sent to The National Archives, where they will be kept for the future of both organisations and may never be destroyed. This is the final phase of a records lifecycle. If you are unsure whether your records have historical value, please get in touch with the Corporate Records Management Team.

7. Record Retention Schedule

7.1. Keeping unnecessary records wastes staff time, uses up valuable space and incurs unnecessary costs. It also imposes a risk liability when it comes to servicing requests for information made under the Data Protection Act 2018 (DPA) and/or the Freedom of Information Act 2000. Moreover, compliance with these acts means that, for example, personal data must not be kept longer than is necessary for the purposes for which it was collected (Principle 5 of the DPA).

7.2. Corporate Records should only be destroyed in accordance with the NHS England and Corporate Records Retention and Disposal Schedule. Primary Care Records should only be destroyed in accordance with the NHS England Primary Care Services Retention Schedule, both of which derive from the NHS Records Management Code of Practice 2021. It can be a personal criminal offence to destroy requested information under either the Data Protection Act 2018, General Data Protection Regulation Article 5 (1e), or the Freedom of Information Act (Section 77). Therefore, both organisations need to be able to demonstrate clearly that records destruction has taken place in accordance with proper retention procedures.

7.3. The Code of Practice on Records Management, issued under Section 46 of the Freedom of Information Act 2000, requires that records disposal 'is undertaken in accordance with clearly established policies that have been formally adopted'. NHS England Corporate Records Retention and Disposal Schedule is a key component of both organisation’s information compliance and allows it to standardise its approach to retention and disposal.

7.4. The recommended retention periods shown on the NHS England Corporate Records Retention and Disposal Schedule apply to the official or master copy of the records. Any duplicates or local copies made for working purposes should be kept for as short a period of time as possible. Duplication should be avoided unless absolutely necessary. It should be clear who is responsible for retaining the master version of a record and copies should be clearly marked as such to avoid confusion.

7.5. Some types of records which may be created and kept locally are the responsibility of the local department, but may be found under a different function on the retention schedule: for example where recruitment is carried out by departments, the department shall be responsible for ensuring the

disposal of the records relating to unsuccessful candidate, this type of record is listed under Human Resources in the retention schedule.

8. Records involved in Investigations, Inquiries, Incidents, Litigation and Legal Holds

8.1. A Legal hold, also known as a litigation hold, document hold, hold order or preservation order is an instruction directing employees to preserve (and refrain from destroying or modifying) certain records and information (both paper and electronic) that may be relevant to the subject matter of a pending or anticipated lawsuit, investigation, incident or inquiry. Organisations have a duty to preserve relevant information when a lawsuit, investigation, incident or inquiry is reasonably anticipated. Staff must immediately notify the Senior Lead for Records Management if they have been notified of a Litigation, Investigation, Incident or Inquiry or have reasonable foresight of a future Litigation, Investigation, Incident or Inquiry as this could result in records being held beyond their identified retention period.

8.2. Following an incident, many internal investigations or legal challenges may be made. These may include Coroners inquests, public inquiries, criminal investigations and civil action. When planning for and responding to an incident it is essential that any decisions made or actions taken are recorded and stored in a way that can be retrieved later to provide evidence.

8.3. The Corporate Records Management team will use this information and log details of the records which have been placed on hold.

8.4. The Legal Hold decision will be determined by the Head of Information Governance / Data Protection Officer.

8.5. When a Legal Hold is terminated, Records previously covered by the Legal Hold should be retained in accordance with the applicable retention period under this policy without regard to the Legal Hold and retained. Non-Records or Records not previously subject to retention may be destroyed.

8.6. The Senior Lead for Corporate Records Management will work alongside NHS England's Inquiry Hub to ensure disclosure of records and information to Public Inquiries.

9. Record Naming and Good Practice

9.1. Record naming is an important process in records management and it is essential that a unified approach is undertaken within all areas of NHS England to aid in the management of records.

9.2. Staff members should refrain from naming folders or files with their own name unless the folder or file contains records that are biographical in nature about that individual, for example, personnel records.

9.3. The NHS England standard naming convention, see Appendix C, must be used for the filename of all electronic documents created by staff members from the implementation date of this policy.

9.4. The re-naming of old documents is optional but new documents must follow the standard naming convention.

9.5. Version Control is the management of multiple revisions to the same document. Version control enables us to tell one version of a document from another. For more guidance on this, refer to Appendix C of this Policy.

9.6. NHS England is making preparations to move away from the Atos platforms and both NHS England have agreed to utilise adopted Office 365 applications

to store data, records and information. In particular, new Collaboration Drives hosted on SharePoint.

The new joint Collaboration Drives should be used as central document repositories for teams, replacing the Atos shared drives. This will ensure that documents are easily accessible, even in the document owner's absence. Documents should be declared in this environment in order to manage retention. More advice and guidance can be sought from the Corporate Records Management Team.

Microsoft OneDrive replaces the Atos P: drive. OneDrive must not be used for the storage of corporate records.

Microsoft OneNote must not be used for the storage of corporate records.

9.7. Where records contain person identifiable data or corporate sensitive information it is a legal requirement that such data is stored securely. You must ensure that you adopt one of two approaches:

- For records stored in Office 365 Document Libraries, site owners must ensure that the security permissions are up to date and appropriate. For further advice contact the ICT team on england.tda@nhs.net
- For NHS England records in shared drives, contact the Atos Service Desk on openservice@atos.net and ask for the folder containing the data to be password protected and access only allowed for specific, named personnel.

9.8. Good record keeping should prevent record duplication. Staff members should ensure team members have not previously created a record prior to initiating a new document.

9.9. Good record keeping requires information to be recorded at the same time an event has occurred, or as soon as possible afterwards.

9.10. Staff members should ensure their handwriting is legible when making entries on paper records.

9.11. Staff members should ensure records are relevant including their opinions about individuals, as the individual has the right gain access to their records via a Subject Access Request under the Data Protection Act 2018.

9.12. Be aware when redacting Microsoft Word documents electronically by using the black highlight text tool as this process is reversible. A Microsoft Word file converted into PDF can be easily read merely by copying if from PDF back into Word. There is professional redaction software in place to redact information, please contact the Corporate Records Team for advice on accessing the software.

9.13. Important and / or business critical information must not be cascaded via instant messaging (e.g. MS Teams Chat, text messages, WhatsApp messages, Signal, Slack). If such information is distributed via instant message, it is the responsibility of those in possession of the information to ensure the information is extracted and saved as a record. This extract must be saved a central document repository on NHS England Office 365 system.

10. Record Maintenance

10.1. Electronic documents and records should be maintained in accordance with this Corporate Document and Records Management Policy.

10.2. At the present time there is no national external data storage organisation for paper records. To keep costs low, and in accordance with our aim to move to become a largely paperless organisation by 2023 NHS England staff are encouraged to save in electronic format wherever applicable. Records which need to remain in paper format are often Incident Log Books, 'Sealed' contract records which are usually identified by an embossed stamp and are executive level. For corporate records which you feel cannot be digitised and require off site storing please contact the Corporate Records Management Team for support and advice.

10.3. The movement and location of paper records should be controlled and tracked to ensure that a record can be easily retrieved at any time. This will enable the original record to be traced and located if required and must be held in a shared location.

10.4. Paper file storage must be secured from unauthorised access and meet fire regulations.

10.5. Information Asset Owners should ensure they have a contingency or business continuity plan to provide protection for records which are vital to the continued functioning of NHS England.

10.6. Records, held in electronic format within the collaboration drives have regular back-up copies scheduled and undertaken on a daily basis via the Corporate ICT Team.

11. Record Access

11.1. There are a range of statutory provisions that give individuals the right of access to information created or held by NHS England such as a data subject access request, Freedom of Information request and correspondence on how a decision was made. The Data Protection Act 2018 allows individuals to find out what personal data is held about them. The Freedom of Information Act 2000 gives the public the right of access to information held by public authorities. The Inquiries Act provides the power to compel an organisation to disclose evidence within the scope of an Inquiry.

12. Record Disclosure

12.1. There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly a range of provisions that require or permit disclosure.

12.2. Only certain staff members have the authority, which is dictated by their role, to disclose records. Staff members with this authority should make a record of any copies of records they have disclosed, and to whom, in conjunction with NHS England's Freedom of Information Policy and NHS England's Procedure for managing personal data requests.

13. Record Closure

13.1. In the case of paper corporate records, they should be closed and retention period applied, as soon as they have ceased to be in active use other than for reference purposes. NHS England's electronic corporate records should be stored in the collaboration drives and retention applied.

13.2. The NHS England's Records Retention and Disposal Schedule is available on the corporate website, and will help you apply timescales to your records to ensure records are not kept longer than necessary.

13.3. If a record is deleted / destroyed once its retention period has been reached, then a Records Disposal Certificate must be completed and saved in order to prove that the record existed, met its retention and was then disposed of. Copies of Disposal Certificates must be provided to the Corporate Records Management team. See Appendix F for a copy of the Record Disposal Certificate. NHS England records from August 2016 until December 2021 were held within the ERMS system, before best practice became to store and declare records on the collaboration drives. For both paper and electronic records, the Record Disposal Certificate at Appendix F now should be used.

14. Record Appraisal

14.1. Appraisal refers to the process of determining whether records are worthy of permanent archival preservation, as certain records created by NHS England may be of historical interest to The National Archives.

14.2. The purpose of the appraisal process is to ensure the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed.

14.3. Appraisal should only be undertaken after consultation with the Corporate Records Management team.

14.4. It is the responsibility of the staff member who is leaving their current post or the organisation, and their Line Manager, to identify as part of the exit procedure specific records that should be retained in line with NHS England's Record Retention and Disposal Schedule. These records should then be transferred securely to the collaboration drives and any non-work-related records disposed of.

15. Records Held and/or Transferred for Archiving Purposes

15.1. Records selected for archival preservation and no longer in regular use by NHS England should be transferred to an archival institution, for example a 'Place of Deposit'. This must be approved by The National Archives and have adequate storage and public access facilities.

15.2. Following implementation of the Constitutional Reform and Governance Act 2010, in particular Part 6: Public Records and Freedom of Information, non-active records are required to be transferred no later than 20 years from the creation date of the record, as required by the Public Records Act 1958.

15.3. The Senior Lead for Corporate Records Management will identify NHS England's Place of Deposit and assist in the transfer of those records identified.

16. Record Disposal

16.1. Disposal is the implementation of appraisal and review decisions and the term should not be confused with destruction. A review decision may result in the destruction of records but may also result in the transfer of custody of records, or movement of records from one system to another.

16.2. Records should not be kept longer than is necessary and should be disposed of at the right time. Unnecessary retention of records consumes time, space and equipment use, therefore disposal will aid efficiency. Staff members must regularly refer to the NHS England Record Retention and Disposal Schedule available on the intranet.

16.3. Unnecessary retention may also incur liabilities in respect of the Freedom of Information Act 2000 and the Data Protection Act 2018. If NHS England continue to hold information which we do not have a need to keep, we would be liable to disclose it upon request. The Data Protection Act 2018 also advises that we should not retain personal data longer than is necessary.

16.4. The accounts (both mailbox and personal folder) of staff members who have left employment with NHS England will be deleted within 30 days unless there are extenuating circumstances, for example, an Employment Tribunal claim or litigation case. This is in line with NHSmail policy, and will ensure best utilisation of our server space, as well as to ensure that records are not held in excess of their retention period. It is the Line Manager's responsibility to notify the ICT Service Desk (NHS England) of accounts that should not be deleted.

16.5. Staff members must seek specialist advice from the Information Governance team when considering destruction of the organisation's records through a commercial third party.

16.6. Staff members must seek specialist advice from the Corporate Records Management Team when considering off-site storage of the organisation's records with a commercial third party.

16.7. Short-lived, ephemeral documents such as telephone messages, notes on pads, post-its etc do not need to be kept as records. If they are business critical, they should be transferred to a more formal document which should be saved as a record and stored and declared within the collaboration drives.

17. Scanning

17.1. For reasons such as business efficiency and/or to address problems with storage space, staff may consider the option of scanning paper records into electronic format. Large scale scanning can be a very expensive option and should only be undertaken after approval of a Business Case by their National Director. Further scanning guidance can be found on the NHS England Records Management page of the intranet here https://nhsengland.sharepoint.com/sites/records/default.aspx

17.2. Staff members involved in a process to scan paper records into electronic format with the purpose of discarding the original paper file, should ensure records are scanned in compliance with the British Standard BS 10008 Evidential Weight and Legal Admissibility of Electronic Information to conform to the provisions of the Records Management Code of Practice and/or seek advice from the Corporate Records Manager.

17.3. By virtue of the Freedom of Information Act 2000, NHS England are required to conform with the British Standard BS 10008:2014 Evidential weight and legal admissibility of information stored electronically.

18. Records Security: Work Base, Home Working, Agile Working

18.1. All person identifiable data or commercially sensitive data must be saved with appropriate security measures.

18.2. Staff must not use home email accounts or private computers to hold or store any sensitive records or information which relates to the business activities of NHS England.

18.3. Removable Media must be NHS England owned and encrypted by the relevant Corporate IT Service. Ideally, person sensitive data should not be stored on any removable media, however if there is no other option ensure

this data is stored on a corporate encrypted device and deleted once transferred to identified secure area folder.

18.4. When printing paper records, especially sensitive documents, ensure appropriate measures have been taken in collecting all documents immediately after printing.

18.5. NHS England have a joint Safe Haven procedure in order to ensure that staff are aware how to receive personal information in a secure manner at a protected point.

18.6. In non-clinical areas, each department should have at least one designated safe haven contact point. Ideally, all information transmitted to the organisation should pass to these contact points. Clinical environments should operate in accordance with safe haven principles and the organisation should operate safe haven procedures for all flows of person identifiable information.

18.7. When transferring data, ensure security measures and precautions have been actioned by the sender and receiver. A robust contract or Service Level Agreement should be in place detailing responsibilities if the information is being transferred to a third party. Please contact the Information Governance team for more advice.

18.8. Never leave your computer screen open when unattended. Always lock it using the keys Control + Alt + Delete and then click on 'Lock This Computer'.

19. Missing and Lost Records

19.1. A 'missing record' is when a record cannot be found or is not available when required.

19.2. In the event of a missing record, a thorough search must be undertaken. This will include initiating a search at the base (this may include facilitating/requesting searches at non- NHS England and locations if appropriate, e.g. GP surgeries or Trust buildings), in addition to reviewing the tracking history of the record.

19.3. If after 5 working days, the record has not been found, the missing record must be reported to Information Governance. The severity of the incident will determine the level of investigation required, and the Information Governance team will complete either the missing record log or incident log as appropriate.

19.4. The missing record should be marked as missing in any electronic / manual tracking systems in use, and the record must be reconstituted, populated as far as possible with all the relevant information and clearly marked as a 'reconstituted record'. If applicable, the electronic / manual tracking system must be updated to note that the record has been reconstituted and on what date this occurred.

19.5. When the original record is located the temporary and original set of records should be merged together. If applicable, the electronic / manual tracking system must be updated to state that the original records were located and merged with the reconstituted record, and with the location of the merged records. Update the Information Governance team with details of when and how the record was found.

19.6. If after 6 months, the record is still missing, it is reasonable to assume that the original set of records has been lost. Inform the Information Governance team.

19.7. Data processors acting on behalf of NHS England are required to develop and maintain local procedures to handle missing records in line with this policy.

20. Distribution and Implementation

20.1. Distribution Plan

20.1.1 This document will be made available to all Staff via the NHS England's intranet site and made available at induction.
20.1.2. A global notice will be sent to all Staff notifying them of the release of this document.
20.1.3. A link to this document will be provided from the Information Governance, Records Management intranet site.

20.1. Training Plan

20.2.1. The Records Management training module forms part of the statutory and mandatory training requirements for all staff across NHS England.
20.2.2. Additional Records Management training is a mandatory aspect of the training programme for all Records and Information Management Coordinators.
20.2.3. Information Governance Training is mandatory for all staff and provided via the Learning Catalogue on ESR.

21. Equality Impact Assessment

21.1. Equality and diversity are at the heart of NHS England's values. Throughout the development of the policies and processes cited in this document, we have given due regard to the need to eliminate discrimination, harassment and victimisation, to advance equality of opportunity, and to foster good relations between people who share a relevant protected characteristic (as cited in under the Equality Act 2010) and those who do not share it.
21.2. As part of its development this document and its impact on equality has been analysed and no detriment identified.

22. Monitoring Compliance with the Policy

22.1. Compliance with the policies and procedures laid down in this document will be monitored via the Corporate Records Management team together with independent reviews by both the internal IG Assurance team and External Audit on a periodic basis.
22.2. The Senior Lead for Corporate Records Management, in conjunction with the Head of Corporate Information Governance is responsible for the monitoring, revision and updating of this document.

Publication Date	Title	Version
May 2018	Freedom of Information Policy	1.02
September 2019	Information Governance Policy	5.1
June 2016	Confidentiality Policy	5.1
September 2019	Data Protection Policy	5.1
September 2019	Information Sharing Policy	4.1

August 2018	Information Security Policy	2.0
March 2019	Information Management Strategy 2019–2021	v1.0
Various dates	NHS England Records Management Procedures and Guidance – available on the intranet at: https://nhsengland.sharepoint.com/TeamCentre/TCO/infogov/Pages/RecordsManagement.aspx	NA
July 2016	Records Management: Code of Practice on Health and Social Care 2016 issued by the Information Governance Alliance https://digital.nhs.uk/information-governance	v1.0

23. Associated Documentation

23.1. The following documents will provide additional information:

Appendix A: Records Management Co-ordinator roles and responsibilities

Champion good records and information management in their team
Act as the first point of contact for uploading records to the collaboration drives at team level by liaising with the requester/ record owner
Act as a first point of contact for records management queries and escalate difficult queries to the Corporate Records Management teams
Advise on the creation and management of folders for their team
Advise their local team to ensure access control is in place for their restricted folders
Attend bi-monthly meetings with the Corporate Records Management teams
Signpost colleagues to the Corporate Document and Records Management Policy and guides on the intranet
Direct colleagues to the Retention & Disposal Schedule / NHS Records Management Code of Practice 2021
Liaise with the Corporate Records Management Teams when there is an information audit or review
Complete the mandatory Records Management training on ESR (available via the catalogue) for NHS England staff and Moodlestaff.

Appendix B: Naming Convention and Version Control

Naming documents and records appropriately is vital to ensure that they can be easily identified and retrieved by those who need them. It is essential that NHS England take a unified approach when naming the documents and records that we hold, as this will aid in the successful management of our records. It is also fundamental that appropriate version control is implemented – this applies regardless of the system you are using to store your documents and records (e.g. in shared drives, MS SharePoint, MS Teams, ~~ORIS,~~ or the collaboration drives)

The following guidance applies to all NHS England records and information, including records such as project and programme records, meeting records and financial records.

Good document titles will consist of the following elements:

Element One: File Title / Description

- The file title should be clear, succinct and descriptive.
- Always make the name of the document or record descriptive of its content or purpose.
- For some file types, it is important to record the date in the file title / description, in particular when saving emails or letters, as the 'sent' date is important to the context of the record, e.g. 20200601 Notice of Closure to Appletree Pharmacy.dox. The date a file was created will also be recorded in the file metadata on MS SharePoint or in the Shared Drive.
- Do not use any ambiguous terms such as 'miscellaneous notes' or 'general information'.
- Do not name the file after the author / creator / owner
- Staff should not use individual names in a file title unless the file is biographical in nature about that individual; for example - personnel records.
- Both SharePoint and Shared Drives restrict the file path lengths (including the path to folders / subfolders) and therefore it is sensible to use acronyms for commonly used words or phrases, e.g.: RM for Records Management, IG for Information Governance, FY for Financial Year. Ensure that any acronyms used are recorded on our Acronym Register

Element Two: Document Status

To effectively control the status of a document, and to enable us to tell whether a document is a draft or final document, it is important to ensure this is indicated in the document name:

- Use DRAFT after the title to indicate draft versions
- Use FINAL after the title to indicate final versions

When renaming a document from DRAFT to FINAL in MS SharePoint, or vice versa, please follow these steps:

- Select the elllipsis next to the title that you would like to update

- Select ‘Rename’
- Rename to DRAFT or FINAL

SharePoint 365 manages the version control of documents for you and this change will be recorded as a minor change, retaining the history of the document. For more information on managing the version history in SharePoint see section 2.0 Version Control.

Networked Shared Drives (e.g. G:\ drive) do not manage version control. When working in shared drives, ensure that the version number of a document is included in the document footer.

- Use whole numbers (e.g. v1.0, v2.0, v3.0) to indicate that the version is final.
- Use decimal numbers (e.g. v0.1, v1.1, v1.2) to indicate that the version is a draft and not finalised yet.

Examples of well named documents

Office 365

- Corporate Document and Records Management Policy FINAL.pdf
- Information Management Strategy DRAFT.docx
- 2018-19 Year End Accounts FINAL.xlsx
- 20200401 Funding Notification to Dr Singh.docx

Networked Shared Drive

- Archiving Records Guidance v2.0 FINAL.pdf
- RIMC Meeting Minutes v0.1 DRAFT.docx
- 2019-20 Annual Budget v0.4 DRAFT.xlsx
- 20191215 CG approval of budget spend.msg

Naming conventions for emails

All the advice and guidance that applies to naming documents and records applies equally to naming emails. However, there are specific elements that staff should be aware of:

- When saving an email, you must change the title of the email if it does not accurately reflect the content
- Do not include ‘email’ as part of the title, as electronic document type extension will show what type of file it is
- Save all emails with their attachments
- Save all emails as Outlook Email Format (.msg)
- Do include the date (YYYYMMDD) the email was sent / received in the title, for example: *20190331 Confirmation of monthly expenditure.msg*

Naming conventions for folders

It is important to use clear, logical and accurate titles for folders. The benefits of providing meaningful titles within the filing structure include:

- The hierarchy of the structure is clearly identifiable by the titles of the folders.
- Peer relationships between folders are clearly identifiable indicating a range of preferred locations for different types of record on a related activity.
- At the lowest level of folders (outlined in the box) it is clear what is expected to be captured into each folder.

The following rules should be followed when naming folders, just as when naming documents and records:

- The file title should be clear, succinct and descriptive.
- Always make the name of the document or record descriptive of its content or purpose.
- Do not use any ambiguous terms such as ‘miscellaneous notes’ or ‘general information’.
- Do not name the file after the author / creator / owner
- Staff should not use individual names in a file title unless the file is biographical in nature about that individual, for example, personnel records

Version Control

As mentioned in section 1.2 Document Status, when working in traditional Shared Drives version control can only be managed by using the version number in the document title. When working in Office365, SharePoint manages the version control of the document saved within it. To view the version history of a particular document, hover your mouse over the specific document – the ellipses should appear, select it:

Now select *Version History*

This will show you the version history of the document and allow you to open any of the previous versions.

However, the version history of a document will only be tracked within the original document. If a document is downloaded and worked on locally, then reuploaded as a ‘new’ document, the version history will become detached and any hyperlinks to the original document will be broken.

Therefore, it is imperative when collaborating or sharing documents that a hyperlink is used, **do not** circulate documents as attachments on emails. This will reduce the risk of duplication, and will manage version control effectively, enabling efficient collaboration between teams. If working remotely and without WIFI, staff can use their Personal Hotspot from their mobile phones to remain connected and negate the need to work offline.

Appendix C: Protective Marking Scheme – Government Security Markings

Classification of NHS Information - Marking Guidance for NHS England

NHS England holds a wide range of information and has a responsibility to manage all information in its care such that risk is minimised; to ensure business continuity and to protect the rights of individuals.

Both organisations are public bodies and as such, classification must follow that laid down by Government. ALL information both organisations collects, stores, processes, generates or shares to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection.

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

Government Security Classifications (updated May 2018) have been implemented to assist you in deciding how to share and protect information. Three simplified levels of security classifications for information assets are now in effect. The new levels are;

Official
This is the default classification for all NHSI documentation. Most organisations operate almost exclusively at this level. It is expected that normal security measures will be enforced through local processes and therefore provide sufficient levels of protection to information ie staff should be sufficiently aware and understand that they have a responsibility for securely handling any information that is entrusted to them.

Official-Sensitive: Personal
Information marked with this classification will be sensitive information relating to an identifiable individual (or group), where inappropriate access could have damaging consequences.

Official-Sensitive: Commercial
Information marked with this classification will be commercial or market sensitive information that could have damaging consequences (for individuals or NHSI) including reputational damage if it were lost, stolen, or inappropriately published.

This simplified procedure will make it easier and more efficient for information to be handled and protected and places greater emphasis on individuals taking personal responsibility for data they handle.

All information used by NHS England is by definition ‘OFFICIAL.’ It is unlikely NHS England will work with ‘SECRET’ or ‘TOP SECRET’ information.
Things to remember about OFFICIAL information:

1. Ordinarily OFFICIAL information does not need to be marked for non-confidential information.
2. 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.

3. This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic documents/records.
4. In additional to the marking of OFFICIAL-SENSITIVE further detail is required regarding the content of the document or record, i.e.:

OFFICIAL – SENSITIVE: COMMERCIAL

Definition - Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to NHS England or a commercial partner if improperly accessed.

Or

OFFICIAL – SENSITIVE: PERSONAL

Definition - Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.

Such documents/records should be marked with the caveat 'OFFICIAL-SENSITIVE: COMMERICAL or SENSITIVE' in capitals at the top and bottom of the page.
In unusual circumstances OFFICIAL – SENSITIVE information may contain both Personal and Commercial data, in such cases the descriptor OFFICIAL – SENSITIVE will suffice.

A Note on Secret / Top Secret Information
On the rare occasion NHS England may receive Secret/Top Secret information, a higher classification level and marking such as 'Secret' or 'Top Secret' must be applied. The information must be password protected if electronic or locked away if paper based. It is important to note that only staff who have a current security clearance through the National Security Vetting process should be allowed to access information that is marked as Secret or Top Secret. Please contact the Corporate Records team for more information.

<u>NHS Confidential</u>
It is worth noting that both NHS Englandstill may receive information which do not have these updated markings applied. Consequently, any information received from an NHS organisation may be marked as NHS Confidential which should then be treated as OFFICIAL – SENSITIVE depending on its type.

<u>How to handle and store OFFICIAL information;</u>
EVERYONE is responsible to handle OFFICIAL information with care by:

- Applying clear desk policy
- 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 the computer
- Using discretion when discussing information out of the office

How to handle and store OFFICIAL – SENSITIVE information;

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, OFFICIAL-SENSITIVE: PERSONAL or OFFICIAL-SENSITIVE: COMMERCIAL material should be stored in a secure encrypted device such as a secure drive or encrypted data stick, lockable room, cabinets or drawers.

- Always apply appropriate protection and comply with the handling rules
- Official-Sensitive Personal and Official-Sensitive Commercial information should be marked prominently with the relevant classification – using the header or footer of a document / record is good practice
- There is no requirement to explicitly mark routine Official information
- The originator / creator is responsible for classifying the information
- It is good practice to place the classification of the information within the subject line of an email if it includes official-sensitive information
- Remember that applying too high a classification can inhibit sharing and lead to unnecessary and potentially expensive protection costs
- Remember that applying too low a classification may result in inappropriate controls and potentially put sensitive information at greater risk of compromise
- Classification can change over time – information can be sensitive but when agreed can be officially published and become 'official' instead
- You do not need to retrospectively classify information – only from the implementation of this guidance
- 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 absolutely necessary
- Send sensitive information by the secure email route or use encrypted data transfers
- 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 cabinet/drawer if paper is used
- If faxing the information, make sure the recipient is expecting your fax and double check their fax number
- Take extra care to be discreet when discussing sensitive issues by telephone, especially when in public areas and minimise sensitive details
- Do not send to internet email addresses e.g. Gmail, Hotmail, etc.
- Only in exceptional cases, where a business need if identified, should sensitive information be emailed over the internet, in an encrypted format, to the third parties. Contact the Corporate Records team for further advice
- The use of pin code or induvial printing passes for secure printing is both widely available and preferable way to manage the printing process

Table 1 – Descriptors that may be used with OFFICIAL-SENSITIVE: COMMERCIAL OR OFFICIAL-SENSITIVE: PERSONAL

Category	Definition	Marking
Appointments	Concerning actual or potential appointments not yet announced	OFFICIAL-SENSITIVE: COMMERCIAL
Barred	Where	OFFICIAL-SENSITIVE: COMMERCIAL

	• there is a statutory (Act of Parliament or European Law) prohibition on disclosure, or • disclosure would constitute a contempt of Court (information the subject of a court order)	
Board	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	OFFICIAL-SENSITIVE: COMMERCIAL
Commercial	Where disclosure would be likely to damage a (third party) commercial undertaking's 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 (even if not yet determined) date	OFFICIAL-SENSITIVE: COMMERCIAL
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
Patient Information	Concerning identifiable information about patients	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

Appendix D: Glossary of Terms

Term of Abbreviation	What it stands for
Assembly	A collection of records. May be a hybrid assembly meaning where electronic and paper records are contained in one folder.
Class	Class is a subdivision of an electronic classification scheme by which the electronic file plan is organised e.g. subject area. A class may either be sub-divided into one or more lower level classes. A class does not contain records. See folder.
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.
Data Quality	Data Quality refers to the procedures and processes in place to ensure that data is accurate, up-to-date, free from duplication (for example, where two or more different records exist for the same individual), and free from confusion (where different parts of a individuals records are held in different places, and possibly in different formats).
Declaration	Declaration is the point at which the document (i.e. record content) and specified metadata elements are frozen so that they cannot be edited by any user, thereby ensuring the integrity of the original data as a complete, reliable and authentic record. The declaration process formally passes the data into corporate control.
Disposition	Manner in which a record is disposed of after a period of time. It is the final stage of record management in which a record is either destroyed or permanently retained.
Document	The International Standards Organisation (ISO) standard 5127/1 states “Recorded information which can be treated as a unit in a documentation process regardless of its physical form and characteristics.”
Electronic Document	Information recorded in a manner that requires a computer or other electronic device to display, interpret, and process it. This includes documents (whether text, graphics, or spreadsheets) generated by a software and stored on magnetic media (disks) or optical media (CDs, DVDs), as well as electronic mail and documents transmitted in electronic data interchange (EDI). An electronic document can contain information as hypertext connected by hyperlinks.
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.
Electronic Records Management System	A system which is designed for the storage and retrieval of Corporate Records.

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 the source of much of the material which constitutes the record. Since records systems tend 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 quality and accountability.
File plan	The full set of classes, folders and records together make up a file plan. It is a full representation of an organisation, designed to support the conduct of the business, and meet records management needs.
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). Folders are allocated to a class.
Information Asset Owner (IAO)	Is 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 that all Information Assets are identified and that the business importance of those assets is established.
Information Asset Administrator (IAA)	Is usually 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 security incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.
Information Lifecycle Management	Information Lifecycle Management is the policies, processes, practices, services and tools used by an organisation to manage its information through every phase of its existence, from creation through to destruction. Record management policies and procedures form part of the Information Lifecycle Management, together with other processes, such as for example, a records inventory, secure storage, records audit etc.
Metadata	Metadata can be defined as data about data. Metadata is structured, encoded data that describes characteristics of a document or record to aid in the identification, discovery, assessment and management of documents and records. Examples of metadata: title, dates created, author, format, etc.
Naming Convention	A naming convention is a collection of rules which are used to specify the name of a document, record or folder.
Place of Deposit	A Place of Deposit is a record office which has been approved by the National Archives for the deposit of public records in accordance with the Public Records Act 1958.
Protective marking	Protective marking is a metadata field applied to an object to show the level of security assigned to the 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.
Record	A record in the records management terminology may not be the same as a record in database terminology. A record for the

	purposes of this document is used to denote a “record of activity” just as a health record is the record of activity of a patients NHS contact. A record may be any document, email, web page, database extract or collection of these which form a record of activity. A record of activity for a database extract may therefore include a collection of health records. A formal definition is “information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business.” (BS ISO 15489.1 Information and Documentation. Records Management
Safe Haven	Safe Haven is the 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.

Appendix E: Record Disposal Certificate

Record Disposal Certificate

Disposal of Records				
Section:	**Name:**		**Date:**	
Title of Record (list all):				
Format (electronic/ paper):				
Reason for disposal:				
Legal hold not placed upon these records:	None			
Method of disposal: (tick relevant box)	Destruction		Transferred to archive	
If destroyed, method of destruction:				
Date of disposal:				
Authority:				
Not subject to current information request: (tick once checked)				

Please complete the form, retain a copy for your own records and send a copy to:

england.ig-corporate@nhs.net

Appendix F: Metadata Standard for Digitised Records

Mandatory Metadata Fields (must be applied to all documents / records)

- Creator
- Date
- Subject
- Title
- Version Number
- Security Classification (Official, Official Sensitive Personal or Official Sensitive Commercial)

Based on best practice guidance available in the e-Government Metadata Standard which was produced by the Cabinet Office. This standard defines how UK public sector bodies should label documents to make information more easily managed, found and shared.

For NHS Improvement, the Business Services Transformation Programme is considering which of these metadata fields could be attached to documents and records automatically. There are some that would still need to be attached manually. Further guidance on metadata will be forthcoming in coming months.

Appendix G: NHSX staff

NHSX brings teams from the Department of Health and Social Care, NHS England together into one unit. A decision was made that all NHSX staff will follow both the NHS England Corporate Document and Records Management Policy and the Corporate Records Retention and Disposal Schedule.

NHSX staff will save their records and information in the information management systems provided by NHSX and follow the principles in both policies to manage their records and information effectively and lawfully, therefore all staff are encouraged to read over both policies for their full understanding.

NHSX staff will be supported by their own Compliance Manager based within NHSX who will be supported by local Records and Information Management Coordinators across directorates and teams to encourage good practice and adherence to the policies.

All policy advice, including but not limited to managing emails, naming and classifying records and information to disposing of expired records should be followed with the only differences being the information management systems and who to contact i.e. NHSX Compliance manager and NHSX ICT department.

Version Control Tracker

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
1.0	January 2019	Head of Corporate Records and Corporate Records Manager	Approved	A new, joint NHS England and NHS Improvement policy created
2.0	September 2019	Head of Corporate Records and Corporate Records Manager		Target Audience and Description updated to include NHSX 3.2 updated to include NHSX 5.9.6 & 5.9.7 updated to reflex organisational move towards Office 365. Appendix C updated to reflect new joint naming convention guidance Appendix H added to reflect the role of NHSX
3.0	June 2021	Senior Lead – Corporate Records Management		Records Management Glossary of Abbreviations and Acronyms removed as appendix and reference added in Section 5.5 to the live Acronym Register Appendix B updated in line with current naming convention and version control guidance. 1.4 Instant Messages added as a record type 2.1 Inquiries Act added 5.7.2 Reference to the Primary Care Retention Schedule added 5.8.6 Added to reflect the role of the new NHSEI Inquiry Hub 5.9.7 Updated to reflect the role of the Collaboration Drives 9.13 Added to reflect the use of instant messaging Roles updated throughout to reflect the role of the Senior Lead – Corporate Records Management
4.0	June 2022	Corporate Records Manager		Moved to a new template format Removed all references to NHS Improvement now all

				organisations under the umbrella of NHS England