North East Ambulance Service NHS
NHS Foundation Trust

Records Management Policy

Document Control Sheet

Q Pulse Reference Number	POL-F-IMT-10
Version Number	V03
Document Author	Information Governance Manager
Lead Executive Director Sponsor	Director of Finance and Resources
Ratifying Committee	Finance Committee
Date Ratified	15 February 2018
Date Policy Effective From	01 March 2018
Next Review Date	01 March 2021
Keywords	Legal obligations, Access to health records, Business critical information, privacy, Personal data, rights, subject access

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

This policy supersedes all previous issues.

Version Control - Table of Revisions

All changes to the document must be recorded within the 'Table of Revisions'.

Version number	Document section/ page number	Description of change and reason (e.g. initial review by author/ requested at approval group	Author/ Reviewer	Date revised
01	All	First issue	IG Manager	Feb 2008
01	All	Reviewed to ensure the policy follows the structure identified in the Organisational-wide Policy for the Development and Management of Procedural Documents and the CNST requirements.	IG Manager	Sept 2008
01	All	Following ratification.	IG Manager	Sept 2009
01	Title	Policy title in Docuviewer changed to match document title and document owner added to profile box.	IG Manager	Nov 2009
01	Review date	Review date changed from 1 year to 2 years	IG Manager	Dec 2011
01	All	Following minor comments made by the Policy Review Group.	IG Manager	Mar 2012
01	E&D and Version control	E&D section moved Document control section moved to end	IG manager	May 2012
01	All	Minor organisation and policy reference updates	IG Manager	May 2014
2	All	Reformatting into new template	IG Manager	Sept 2016
3	All	Policy Reviewed Section RMCOP refreshed to suggest new location	IG Officer	March 2017
3	All 4 5 8 9.2	Full review in line with GDPR and UK Data Protection Act. Update of responsibilities. Definition of 'documents' and 'record'. Updated. Addition of monitoring of NEAS07's.	IG Manager	Oct 2017
3	Appendix B Section 9	Retention periods updated to refer to Records Retention Schedule and Email Policy. Monitoring section strengthened.	Finance Committee	Feb 2018

This page should not be longer than one single page.

Table of Contents

1. Introduction

Records management is vital to the delivery of our services in an orderly, efficient, and accountable manner. Effective records management will help ensure that we have the right information at the right time to make the right decisions. It will provide evidence of what we do and why, therefore protecting the interests of the North East Ambulance Service NHS Foundation Trust (Trust), staff and all who interact with the Trust.

Records, and the information they preserve, are an important corporate asset. We will create and manage records efficiently, make them accessible where possible, protect and store them securely and dispose of them safely at the right time.

The nature of the work undertaken by the Trust brings us into possession of a great deal of confidential, and often highly sensitive information, both patient and staff related. Therefore, it is essential that the public at large have confidence that the organisation as a whole maintains confidentiality of information in whatever form it is given, to whoever it is given and for whatever purpose.

Records and documents are different. Documents consist of information or data that can be structured or unstructured. Records provide evidence of the activities of the Trust’s 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.

The Trust is a data controller with obligations set out in the Data Protection Act and a public authority with obligations under the Freedom of Information Act 2000.This policy respects and complies with the applicable laws and standards including (but not limited to):

- UK Data Protection Legislation
- EU General Data Protection Regulation 2016
- Access to Health Records 1990
- The Public Records Act 1967
- The Re-use of Public Sector Information Regulations 2005
- Department of Health Records Management: NHS Code of Practice
- BS ISO15489 – Records Management

2. Purpose

This policy outlines the Trusts approach to records management. By adopting this policy we aim to ensure that the record, whatever form it takes, is accurate, reliable, ordered, complete, useful, up to date and accessible whenever it is needed

The policy covers the management of records and not the detailed requirements of what a record should contain for either corporate or clinical use. For guidance on these matters see departmental policies/procedures.

3. Scope

This policy covers all sites and systems operating and utilised by the Trust.

The policy applies to any individual employed, in any capacity, by the Trust, and any volunteer or contractor who holds a Trust domain account.

This policy relates to the management of all documents and records, in all technical or physical formats or media, created or received by the Trust in the conduct of its business activities.

4. Duties - Roles & Responsibilities

4.1 Trust Board

The Trust Board is collectively responsible for ensuring that the information risk management processes are providing them with adequate and appropriate information and assurances relating to risks against the Trust’s objectives.

4.2 Chief Executive

The Chief Executive is ultimately responsible for the confidentiality and security of patient, staff and corporate information. Implementation of, and compliance with the policy is delegated to the Director of Finance and Resources.

4.3 Director of Finance and Resources

The Director of Finance and Resources who is also the Senior Information Risk Owner (SIRO) is the sponsor of this policy and has overall responsibility for the development and regular review of policies within their areas of responsibility.

4.4 Caldicott Guardian

Director of Quality and Safety (Executive Nurse) is also the Caldicott Guardian who has responsibility for:

- Reflecting patients’ interests regarding the management and use of their records.
- Ensuring patient identifiable information is stored and shared in an appropriate and secure manner in line with the Caldicott Principles.

4.5 Information Governance Manager

Has responsibility for:

- Developing, maintaining and implementing this policy.
- Work with line managers and information asset owners in the investigation of potential breaches of this policy.
- Implement secure processes to protect personal information transferred electronically.

- Report any risks related records management to the SIRO and Caldicott Guardian.

4.6 Information Asset Owners

The Information Asset Owers (IAOs) are responsible for ensuring this policy is adhered to and for developing their own local guidance for records management in their area of responsibility. They are assisted in the day to day operational tasks by Information Asset Administrators (IAAs).

4.7 All staff

Under the Public Records Act, all NHS employees have responsibility for any records that they create or use. Any records created by an employee of the NHS are public records and are subject to both legal and professional obligations. These legal and professional obligations limit, prohibit, or set conditions in respect of the management, use and disclosure of information.

Similarly the Trust is subject to a range of statutes that permit or require information to be used or disclosed. Additionally, clinicians are obliged to meet records management standards set by their governing bodies.

5. Glossary of Terms

This policy uses the following terms:

Term	Description
Documents	Recorded information which can be treated as a unit in a documentation process regardless of its physical form and characteristics.
Information	The Trust's records are important sources of administrative, clinical, evidential and historical information. They are vital to the Trust to support its current and future operations, for the purpose of accountability (including meeting the requirements of Freedom of Information (FOI) legislation), and for an awareness and understanding of its history and procedures
Record	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.
Records Lifecycle	Describes the life of a record from its creation / receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.
Records Management	Is described in the NHS Records Management Code of Practice as 'the efficient and systematic control of the creation, receipt, maintenance, use and disposition of

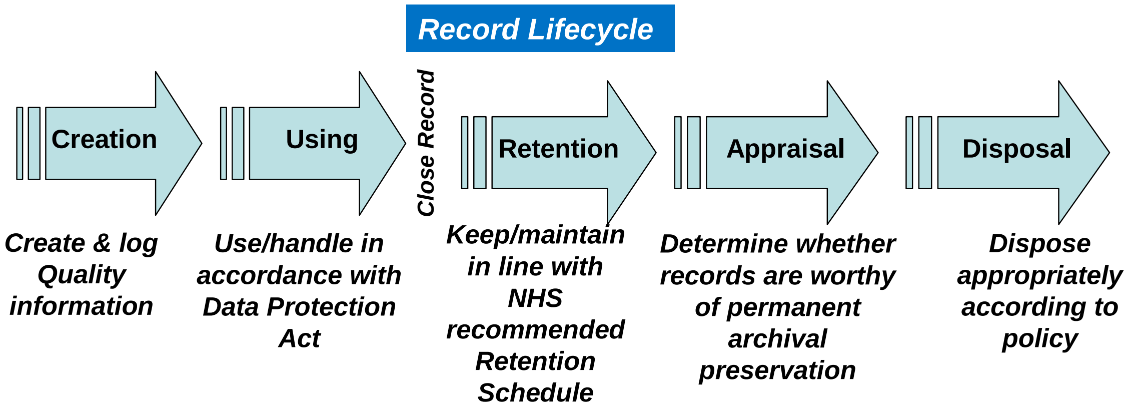
Term	Description
	records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records'.

6. Policy Content

6.1 Standards of Records Management

From the moment a record is created or received, the Trust must ensure that:

- The quality and quantity of information it generates is controlled.
- The information is maintained in a manner that effectively services the needs of the organisation and its stakeholders.
- The information is disposed appropriately when it is no longer required.


Record Lifecycle
Creation
Using
Close Record
Retention
Appraisal
Disposal
Create & log Quality information
Use/handle in accordance with Data Protection Act
Keep/maintain in line with NHS recommended Retention Schedule
Determine whether records are worthy of permanent archival preservation
Dispose appropriately according to policy

IAOs are responsible for developing their own local procedures relating to the records they have a responsibility for. Appendix A provides some guidance on what should be contained in the local procedures.

6.1.1 Record creation

In the creation of a record, consideration must be given to what is being recorded, how it is being recorded and why. This is to ensure that the records which are created are not only adequate and consistent but necessary for statutory, legal and business requirements.

Records created by the Trust should be arranged in a record keeping system that will enable the Trust to obtain the maximum benefit from the quick and easy retrieval of information. This will include a set of rules for referencing, titling, indexing and, if appropriate, security marking records which are easily understood and enable the efficient retrieval of information.

6.1.2 Master record

Thanks to the ease with which new records can be created, copied and circulated, it is inevitable that multiple copies of records will still exist. For example, all members of a committee each receiving their own copies of the minutes and associated papers.

Identify the agreed source of the master copy (for example the copy of the minutes signed by the committee chair, or the project sponsor's version of the Project Plan).

Document authors should consider establishing procedures for ensuring the capture of the master copy. This should include a statement regarding whether the paper or electronic version of records is to be the master copy (where appropriate).

6.1.3 Storage of records

The following factors should be taken into account when considering how records will be stored:

- Security of the records.
- Health and safety requirements.
- Access requirements (i.e. how accessible does the record need to be).
- The type of record being stored and its environmental requirements (e.g. electronic storage media should not be placed in close proximity to strong magnetic fields).
- The choice of media should be based on consideration of practicality and costs.

6.1.4 Paper Records

Records must be stored in a way that allows the information contained within them to be available when they are needed, where they are needed, and by the person who needs them. The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with and that there is an auditable trail of these record transactions.

Current records should be stored in the business area adjacent to users held in a secure location when not being used e.g. lockable filing cabinets, cupboards, rooms (locked and / or alarmed when out of normal working hours). Storage locations should be clean and tidy with proper environmental controls and adequate protection against fire and flood and should provide a safe working environment for staff.

Records should be closed as soon as they have ceased to be active for use other than reference. Where records are no longer required for the conduct of current business their placement in a designated storage (place of deposit) area with specified destructions dates is more economical and efficient. These must be controlled via formal contracts that clearly stipulate storage, security and retrieval requirements.

6.1.5 Electronic Records

Electronic records may be contained within specific applications or in a file directory. The electronic storage medium should consider:

- Storage and back-up.
- Access.
- Folder designs, including security controls, to be approved by the record owners.

6.1.6 Other Media

In the case of photographs, the quality of the images available from negatives or original prints should be considered and new prints may be made in cases where the original is deteriorating. Film should be stored in dust-free metal cans and placed horizontally on metal shelves.

Sound recordings and video recordings (e.g. tapes and DVDs) should be stored in metal, cardboard or inert plastic containers, and placed vertically on metal shelving.

6.1.7 Scanning

The option of scanning paper records into electronic format may be considered for reasons of business efficiency, to address problems with storage space or to include a record of a paper document within an existing electronic record. Where this is proposed, it should be in line with the British Standards Institutions code of practice of Evidential Weight and Legal Admissibility of Electronic Information (BS 10008:2014).

6.1.8 Archiving Records

A review should be made of the records to determine whether records should be selected for preservation, retained or disposed.

Asset owners should determine whether records which have been retained for the minimum required period are to be selected for permanent preservation, destroyed or retained by the Trust basing their decisions on the need to preserve records which may be of value to future employees or influenced by local factors such as ongoing research. Records identified for permanent preservation must be transferred to the appropriate repository e.g. the County Archive or Public Records Office.

6.1.9 Disposal of Records

Asset owners are responsible for making sure that all records are periodically and routinely reviewed to determine what can be disposed of or destroyed in the light of local and national guidance.

In respect of health records, it is recommended that a multi-disciplinary Health Records Committee and / or Health Records User Group should be established to provide advice on local policy, particularly for the retention, archiving or disposal of sensitive personal health records.

The specified periods define when a review should be made of the records to determine whether records should be selected for preservation, retained or disposed of bearing in mind that the destruction of records is an irreversible act but the cost of keeping them is high and ongoing.

Where a record type is not listed in the retention schedule, IAOs should consider how other organisations manage these record types and should carry out a risk assessment of the pros and cons of destroying the record or maintaining it for a prolonged period in order to decide how best to manage the record.

Attention should also be paid to other retention periods for similar record types. The decision process around why a particular record type may be maintained or destroyed should be clearly documented.

Where the need for disposal has been identified secure destruction of the record must be carried out as many Trust records contain sensitive and / or confidential information.

The normal destruction method for sensitive / confidential paper records used within the Trust is shredding, undertaken by an approved contractor. There must be a formal contract between the contractor / supplier and the Trust which details the security and confidentiality requirements associated with the transportation and destruction of confidential information. Non sensitive / confidential papers records can be put in the recycling bins. Secure destruction of electronic records will be undertaken by IT experts within the Trust.

Record owners should compile a register of records which have been destroyed providing details of the type of record, when it was destroyed and by whom and should be retained by the relevant department for 30 years.

If records or documents are disposed of, in error, before the end of their retention period, it should be clearly marked on the register as “Disposal within minimum retention period” and an incident form should be completed, so that the risks associated with inappropriate disposal can be assessed and managed, and any necessary actions can be taken.

If it is found that records have been deliberately and inappropriately disposed of, or otherwise altered, to prevent lawful access under the DPA, FOI or other relevant legislation, the parties responsible will liable to disciplinary action (under the Disciplinary Policy) and may also be liable to criminal prosecution.

6.2 Disclosure and public access to records

If the Trust receives a request for access to a record or document that is due for disposal, the normal procedure for processing access requests will be followed.

No member of staff should dispose of a record – even if its retention period has expired - if they are aware that it is subject to an information request, until they have been advised by the relevant department that the processing of the request has been completed (including the appeals process, if appropriate).

6.3 Policy Specific to Emails

E-mail is an essential tool for and in many instances forms the only record of a decision or action taken. There are legal obligations to manage records (including emails) effectively. Without appropriate management there is a risk that important business records are lost and sensitive or confidential information is inadvertently disclosed.

Email correspondence can be thought of as the short-term correspondence that should be regularly deleted. Email records are more important if they record a decision, action or policy and should be managed professionally in the same way as other records. Further information is provided in Appendix B.

6.4 Retention Schedules

The records retention schedules within the Department of Health Records Management: NHS Code of Practice provide information about all records commonly found within the Trust. For ease of use, there are separate schedules relating to health and corporate (i.e. non-health) records. The retention schedules apply to all the records concerned, irrespective of the format (e.g. paper, databases, e-mails, photographs, CD-ROMs) in which they are created or held.

Type of record: lists alphabetically records created as part of a particular function. The business and corporate records schedule has grouped together records of major functions commonly found in NHS organisations.

Minimum retention period: records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If records need to be kept longer than the recommended minimum period, then the period can be varied accordingly with the decision and the reasons behind it, on its own retention schedule. Records selected for permanent preservation by the relevant place of deposit should normally be transferred there as soon as they reach the retention period specified and in any case before they reach 30 years old, unless a longer operational retention period is specified in this schedule, in which case transfer should take place as soon as possible after this period has been reached. NHS organisations wishing to keep records more than 30 years old for operational reasons beyond the minimum period specified in this schedule should consult The National Archives for advice.

Derivation: notes the details of legislation and any other references of relevance to the recommended minimum retention period.

Final action: at the end of the relevant minimum retention period, one or more of the following actions will apply:

- Review: records may need to be kept for longer than the minimum retention period due to ongoing administrative need. As part of the review, the organisation should have regard to the fifth principle of the DPA, which requires that personal data is not kept longer than is necessary. If it is decided that the records should be retained for a period longer than the minimum (provided that this does not total a period of 30 years or more from creation, in which case see the comments on the minimum retention period above), the internal retention schedules will need to be amended accordingly and a further review date set. Otherwise, one of the following will apply:

- Transfer / consult a Place of Deposit or The National Archives (see ‘Archives’ section below): if the records have no ongoing administrative value but have or may have long-term historical or research value, or they have some administrative value but are more appropriately held as archives. Records with such value must be transferred to the organisation's approved Place of Deposit. Where the organisation has no existing relationship with a Place of Deposit, The National Archives should be contacted in the first instance. Where an organisation is unsure whether records may have archival value, The National Archives or the Place of Deposit with which the organisation has an existing working relationship should be consulted.

- Destroy: where the records are no longer required to be kept due to statutory requirement or administrative need and they have no long-term historical or research value. In the case of health records, this should be done in consultation with clinicians in the organization.

6.5 Retention periods

As previously stated, records should not ordinarily be kept for longer than 30 years. The Public Records Act does, however, provide for records, which are still in current use to be legally retained. Additionally, under separate legislation, records may be required to be retained for longer than 30 years (e.g. Control of Substances Hazardous to Health Regulations).

Also, in respect of any records that contain personal data as defined by the Data Protection Regulation, consideration should be given to the principle that 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'.

Consideration should also be given Goddard Inquiry. Records relating to child sexual abuse (CSA) must be preserved. Further advice can be sought from the Safeguarding Team.

6.6 Records Audits

An effective records management programme depends on the knowledge of what records are held, in what form they are accessible and their relationship to organisational functions. An information audit has been undertaken to establish a Trust wide information asset register so as to meet this requirement as well as to help promote control over the records and provide valuable data for developing records appraisal and disposal procedures.

7. Training Required for Compliance with this Policy

All staff to receive Mandatory Information Governance Training on an annual basis.

8. Equality and Diversity

The Trust is committed to providing equality of opportunity. We aim to give people the freedom to flourish and develop in an environment free from discrimination, harassment, bullying and prejudice where their contributions, skills and knowledge are recognised and embraced.

We want to ensure that we provide services and employment opportunities that consider and are tailored to peoples' specific needs. Further details or our aims and objectives are outlined in our Equality Strategy – One Service for All.

We use the NHS England's Equality Delivery System 2 as our framework to monitor and improve our performance on equality and inclusion. We have also made a commitment to the Job Centre Two Ticks about Disability scheme, the Stonewall Work Place Equality Index meet our mandated requirements in relation to the Workforce Race Equality Standard and support a range of other initiatives.

This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly.

The Trust values and respects the diversity of its employees and the communities it serves. In applying this policy we have considered eliminating unlawful discrimination, promoting equality of opportunity and, promoting good relations between people from diverse groups. Any issues highlighted in the assessment have been considered and incorporated into the policy and approved by the Head of Service/Director and relevant committee.

9. Monitoring Compliance with and Effectiveness of this Policy

9.1 Compliance and Effectiveness Monitoring

Arrangements for the monitoring of compliance with this policy and of the effectiveness of the policy are detailed below.

Monitoring Criterion	Response
Who will perform the monitoring?	Information Governance Manager
What are you monitoring?	Records kept beyond retention period. Records recorded as lost/missing/stolen. Records disclosed in error.
When will the monitoring be performed?	Undertaking an annual review of records held offsite. When incidents occur.
How are you going to monitor?	Incidents reports from Ulysses.
What will happen if any shortfalls are identified?	Recorded in the relevant record keeping system relating to the record type. Record on risk register.
Where will the results of the monitoring be reported?	Information Governance Working Group.
How will the resulting action plan be progressed and monitored?	Assessment of the risk with the IAO and report back to the working group.
How will learning take place	Recommendations from the working group and identifying any additional training or changes in process.

9.2 Compliance and Effectiveness Monitoring Table for this policy

Process in the policy	Monitoring and audit					
	Key Performance Indicators (KPI)/ Criteria	Method	Who By	Committee	Frequency	Learning/ Action Plan
Compliance with Trust policy template, format and ratification process	• Style, format and template • Explanation of terms used • Consultation process • Ratification process • Review arrangements • Control, including archiving arrangements • Associated documents • Supporting references • Monitoring section in policy	Assessing all new and reviewed policies against the guidance through presentation to relevant approval groups	Author and approval groups	Finance Committee	Ongoing	To be developed as necessary
Monitoring and reporting on policy compliance	• Records retained past retention period • Breaches in handling of records	• Report from Trust archiving system • NEAS07 incidents	Information Governance Manager	Information Governance Working Group	Bi-monthly	• Additional training to staff. • Further audit of department concerned.

10. Consultation and Review of this Policy

This policy has been reviewed in consultation with the Information Governance Working Group. The Policy will be reviewed every three years unless there are significant revisions to be made.

11. Implementation of this Policy

This Policy is to be implemented Trust wide through staff briefings, newsletters, team brief, divisional meetings.

12. References

This document refers to the following guidance, including national and international standards:

- UK Data Protection Legislation http://www.legislation.gov.uk/ukpga/1998/29/contents
- EU General Data Protection Regulation 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- Freedom of Information Act 2000 http://www.legislation.gov.uk/ukpga/2000/36/contents
- Access to Health Records 1990 https://www.legislation.gov.uk/ukpga/1990/23/contents
- The Public Records Act 1967 https://www.legislation.gov.uk/ukpga/1967/44/contents
- The Re-use of Public Sector Information Regulations 2005 https://www.legislation.gov.uk/uksi/2005/1515/contents/made
- Department of Health Records Management: NHS Code of Practice https://digital.nhs.uk/codes-of-practice-handling-information
- BS ISO15489 – Records Management https://www.iso.org/standard/62542.html

13. Associated Documentation

This policy refers to the following Trust documents:

- Disciplinary Policy – POL-WOD-HR-7

14. Appendices

Appendix A: Local Records Procedures

Local procedures should include the following information:

- Roles and responsibilities
- List of records covered
- Location of records
- Access to records
- Retention and disposal schedule
- Review and audit of records.

Appendix B: Email Records

E-mails created for the purpose of Trust business should be considered as a formal means of communication and potentially important records. All staff have a responsibility to create, capture and destroy emails appropriately. It is important that email records are actively managed to ensure that they remain accessible, comply with legislation and do not use unnecessary server space.

E-mails should be organised in the same way as other records. They should be filed, retained and destroyed as necessary. The value of each email depends upon its content, therefore emails should be managed differently according to the content of the message e.g. important investigation related messages may be put in the investigation file, other records may be filed accordingly.

E-mail can form a contractual obligation. You need to be aware of this if you enter into an agreement with anyone, especially external contractors.

Email *records* should be managed in line with retention schedules whilst email *correspondence* should be routinely deleted. In determining which emails are actually records you should consider if the message:

- Contains information which documents Trust decisions, including the discussion showing how the decision was arrived at.
- Documents the formulation and execution of policy.
- Contain information upon which Trust business decisions will, or are likely to be based.
- Commit the Trust or its staff to certain courses of action including the commitment of resources and provision or purchase of goods or services.
- Document the establishment, negotiation and maintenance of business relationships with patients, staff or other organisations.
- Record contractual undertakings entered into by the Trust.
- Have long term value for future reference or historical purposes.
- Is covered by a Retention Schedule.

Is it needed to:

- Prove a business related event or activity did or did not occur?
- Demonstrate the initiation, authorisation or completion of a business transaction?
- Identify who took part in a business activity?
- Satisfy legal/compliance purposes?

- Facilitate business analysis and reporting?
- Display public accountability for policies or decisions?

If the answer to any of these is yes, it is likely that the email is a record.

When determining who has responsibility for capturing and keeping the "official" copy of an email record, the following conventions should be observed. Please note: This is a general rule to which there may be exceptions.

For internal (i.e. staff to staff) email records sent or received:

- The sender or initiator of the dialogue forming a message string is responsible for keeping.
- If action is required by recipients, or the recipient is responsible for keeping the record on the matter communicated, they should also keep a copy.

For email records sent externally:

- The sender is responsible for keeping.

For external email records received:

- By one person – the recipient is responsible for keeping
- By multiple recipients – the person responsible for the area of work relating to the message is responsible for keeping e.g. a committee secretary circulating minutes will be the owner and therefore responsible for retaining a copy, a member of collating a Freedom of Information request will retain a copy.
- All other duplicate copies of record email messages can be deleted by users when no longer needed.
- In a string of emails it is normally sufficient to keep only the last email sent as long as it contains all previous emails which are complete and have not been edited.

Where an email is being used to circulate an attachment, it is unlikely that the email itself will be part of the record (unless it is required as evidence that the record was sent at a particular time), it is more likely that the attachment itself is the formal record and the creator would normally be the owner and responsible for its retention.

The following table provides a sample of email categories that are likely to be email records, the list is not exhaustive.

Category	**Examples**
Formal Agreements	Approval of contracts, project plans, policies, strategies

Decisions/confirmation of action	Approval to spend money or carry out a particular activity
Confirmation of completion	Project sign off, receipt of goods
Invoices/purchase order	
External enquiries	Complaints, enquiries, requests for information

The following table provide a sample of email categories that are **unlikely to be email records,** the list is not exhaustive.

Category	**Examples**
'For Information' / Short term reference	News in Brief, updates on building works/maintenance issues
External circulars / Marketing	Mailing list correspondence
Circulated papers for meetings/committees	Copies of meeting papers/minutes (these should be retained by the secretary of the group only)
Draft documents for comment	The author should retain appropriate copies)
Meeting arrangements	Room bookings
Personal messages	Invitation to lunch

When to File Email Records

Emails which need to be retained in line with the NHS Records Retention Schedule should be captured and filed as soon as possible. Email exchanges often result in elongated dialogues stretching over a period of time. This presents a problem in determining the point at which to capture and file a record email. It is not necessary to wait until the conclusion of the dialogue if it is likely to continue over a long period. You should capture the message and file it at significant points in the discussion, deleting all previous messages in the string.

Where to File Email Records

Email messages which are records and need to be kept should be moved out of the email system into a departmental/sectional record keeping system where they are kept in one place with all related records and accessible to all staff working in the same business area. This should be done, preferably by saving to electronic folders within an electronic filing system on an appropriate network shared drive.

If the email is a record, but does not need to be stored as per the Records Management Policy, it should be kept within the email system and filed in appropriate email folders which mirror any existing file and folder structures in your paper and electronic record keeping systems. It should be deleted promptly as soon as no longer required and in any event in line with the Records Retention Schedule.

If the email is a record which needs to be kept for longer than six months, but less than 1 year, it should be moved out of the email system into a suitable backed up record keeping system. If printing the message you should ensure that all header information (sender, recipient, date, subject) are displayed on the printout. Storage of emails in their original electronic format is preferred as this ensures that all the metadata (embedded information about the message) is captured and preserved. This approach also ensures that emails are kept together with all other electronic records relating to the same matter.

Deleting e-mails

E-mails should not be retained indefinitely, most do not need to be kept beyond the timeframe of the subject to which they refer. Exchange will automatically archive emails in line with the Email Policy.

Archiving does not delete the records and should not be used as a substitute for formal retention and destruction procedures.