NHS
Central East
Integrated Care Board

Records Management & Lifecycle Policy

Document Status:

This is a controlled document. Any printed or downloaded copies are not controlled. The version of this document published on the Central East Integrated Care Board website is the controlled copy www.centraleast.icb.nhs.uk

Sustainable Development - Environmental

Do you really need to print this document?

Please consider the environment before you print this document and where possible copies should be printed double-sided. Please also consider setting the page range in the print properties, when relevant to do so, to avoid printing the document in its entirety.

Document Control

Document Owner	Associate Director of Data Security and Information Risk (& Data Protection Officer)
Document Author(s)	Data Security & IG Officer
Directorate	Strategy, Planning and Evaluation
Approved By	CE ICB Board
Date of Approval	1.4.2026
Date of Next Review	31.3.2028
Effective Date	1.4.2026

Version Control

Version	Date	Reviewer(s)	Revision Description
1.0	1.4.2026	ICB Board	Approved

Contents

1. Introduction

1.1 This policy sets out the principles and requirements for Records Management and Lifecycle within NHS Central East Integrated Care Board (ICB). It aims to ensure a consistent and effective approach that supports the organisation's objectives, complies with statutory and regulatory requirements and promotes best practice.

1.2 Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, through every phase of its existence, from their creation, all the way through their lifecycle to their eventual disposal.

1.3 All NHS records are public records under the Public Records Act 1958. This provides statutory obligations upon the ICB to comply with the legal requirements in relation to the records it holds, including, UK General Data Protection Regulations (GDPR), Data Protection Act 2018, Access to Health Records Act 1990, The Freedom of Information Act (FOI) 2000 and Environmental Information Regulations 2004.

1.4 The implementation of the GDPR requires better records management. Organisations need to know what personal data they hold, to be able to tell individuals how long they will keep it for, to be able to access it when they need to, and to keep it securely. This Records Management & Lifecycle Policy aids compliance with GDPR and UK Data Protection Act 2018.

1.5 NHS Records Management Code of Practice has been published by the Department of Health as a guide that sets out the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

1.6 The ICB's records are our corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision making, protect the interests of the ICB and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in uniform and equitable ways. They are a valuable resource because of the information they contain and support the delivery of high quality evidence based healthcare.

1.7 Information has most value when it is accurate, up to date and accessible when needed, good data quality is essential and the availability of complete, accurate, relevant,

accessible and timely data is important in supporting patient care, clinical governance, management of contracts for healthcare planning and accountability.

1.8 The ICB has written this Records Management and Lifecycle Policy and is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

- Better use of physical and server space;
- Better use of staff time;
- Improved control of valuable information resources;
- Compliance with legislation and standards;
- Reduced costs;
- Data quality;
- Archiving and Disposal.

1.9 The ICB also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated corporate function.

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

1.11 It is the responsibility of all staff, including those on temporary or honorary contracts, agency staff and students to comply with this policy.

2. Purpose and Scope

2.1 The purpose of this policy is to ensure that:

- **Records are available when needed** - from which the ICB is able to form a reconstruction of activities or events that have taken place.
- **Records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use and that the current version is identified where multiple versions exist.
- **Records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process and how the record is related to others.

- **Records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process and its integrity and authenticity can be demonstrated.
- **Records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.
- **Records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosures are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as they are required.
- **Records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value.
- **Staff are trained** - so that all staff are made aware of their responsibilities for recordkeeping and management.

2.2 This policy applies to all NHS Central East ICB staff, Board members, contractors, and others involved in undertaking duties for or on behalf of the ICB, such as staff covered by a letter of authority/honorary contract, work experience or any third party authorised to undertake work on behalf of the ICB.

2.3 This policy relates to all clinical and non-clinical records held in any format by the ICB. A record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees, including but not limited to:

- Administrative records (including e.g. personnel, financial, accounting, contracts, litigation, complaints, estates, policies etc);
- Patient health records, including those concerning all specialties, but excluding GP medical records (Guidance for GPs set out in HSC 1998/217) and includes private patients seen on NHS premises;
- Emails and other electronic communications (e.g. MS Teams)
- Any type of audio and video recordings, including physical media such as cassettes and CD-ROMs and digital media such as MS Teams recordings;
- Computer databases, output, and disks, and all other electronic records;
- Photographs, slides and other images;
- Scanned documents;
- Any portable media containing information, such as USB sticks;
- Material intended for short term or transitory use, including notes and “spare copies” of documents;
- Meeting papers, agendas, formal and informal meetings including notes taken by individuals in notebooks and bullet points are all subject to the above; and emails and other electronic communications.

This list is not exhaustive and does not include copies of documents created by other organisations that are kept for reference and information only.

2.4 Limitations and Applications for ICB Staff - The introduction of the Health and Social Care Act 2012 removed some of the powers and rights of commissioning organisations to obtain, handle, use and share confidential and identifiable information from the ICB. In general, ICB staff are not entitled to use Personal Confidential Data (PCD). Whilst this policy and procedure references health records, this advice is only applicable to ICB staff who have a legal right to this information and it is not applicable to all staff.

2.5 A document becomes a record when it has been finalised and becomes part of the organisation's corporate information.

3. Definitions

3.1 **Records management** is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the ICB and preserving an appropriate historical record. The key components of records management are:

- Record creation;
- Record keeping;
- Record maintenance (including tracking of record movements);
- Access and Disclosure;
- Closure and Transfer;
- Appraisal;
- Archiving and Disposal.

3.2 **Records life cycle** 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.

3.3 **Records** are defined as 'recorded information, in any form, created or received and maintained by the ICB in the transaction of their business or conduct of affairs and kept as evidence of such activity'.

3.4 **Information** is a corporate asset. The ICB records are important sources of administrative, evidential and historical information. They are vital to the ICB to support its current and future operations (including meeting the requirements of Freedom of

Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

3.5 **Personal Data** is information which relates to a living individual who can be identified from those data and includes any expression of opinion about the individual. Typical examples could include:

- Person's name, address, full postcode, date of birth
- Email address and telephone numbers
- Pictures, photographs, videos, audio-tapes or other images of patients

3.6 **Public records** – Records of NHS organisations are public records in accordance with Schedule 1 of the Public Records Act 1958.

3.7 **Corporate/business records** are defined as anything that contains information in any media, which has been created or gathered as evidence of undertaking of work activities in the conduct of business. Corporate records may also be generated through supporting patient care and can also be generated through agency/casual staff, consultants and external contractors. Corporate records types may include:

- Administrative records (including personnel, estates, financial and accounting, contract records, litigation and records associated with complaints handling)
- Registers and rotas
- Office/appointment diaries
- Photographs, slides, plans or other graphic work (not clinical in nature)
- Any type of Audio and video tapes
- Records in all electronic formats including emails

These records will support the ICB with a number of key statutory requirements, including:

- Provision of an accurate account of the planning the delivery and evaluation of care;
- Clinical liability;
- Parliamentary accountability;
- Purchasing and contracting, or service agreement management;
- Financial accountability;
- Disputes or legal action;
- Support to Freedom of Information
- Demonstrating sound clinical, information and corporate governance.

All records created in the course of the business of the ICB are corporate records and are public records under the terms of the Public Records Acts 1958 and 1967. This includes email messages and other electronic records (whether business or private email address is used) and are subject to release for FOI and Subject Access / Access

to Health Record requests. (See NHS Mail Data Retention and Information Management Policy November 2022).

3.8 A **health record** is defined as being any record which consists of information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of the individual.

3.9 **Data Quality** is the ability to supply accurate, timely and complete data, which can be translated into information, whenever and wherever this is required. Data quality is vital to effective decision making at all levels of the organisation.

- Data quality incorporates the following attributes:
- Complete (in terms of having been captured in full)
- Accurate (the proximity of the figures to the exact or true values)
- Relevant (the degree to which the data meet current and any potential users' needs)
- Accessible (data must be retrievable in order to be used and in order to assess its quality)
- Timely (recorded and available as soon after the event as possible)
- Valid (within an agreed format which conforms to recognised standards – either national or local)
- Defined (understood by all staff who need to know and reflected in procedural documents)
- Appropriately sought (in terms of being collected or checked once during an episode)
- Appropriately recorded (in either paper or electronic format)

For further definitions relating to Information Governance, please refer to the Data Protection Policy.

4. Policy Statement

4.1 NHS Central East ICB is committed to ensuring compliance with all relevant legislation and best practice in Records Management.

4.2 The ICB will conduct an annual assessment of its compliance against the assertions which make up the Data Security and Protection Toolkit (DSPT) and have the evidence provided for the assessment further assessed by its internal auditors.

4.3 The ICB will conduct periodic reviews to ensure the way it manages its records is in line with statutory obligations and NHS standards.

4.4 All staff are expected to adhere to the requirements set out in this policy.

5. Roles and Responsibilities

5.1 The ICB recognises it has responsibility for ensuring it meets its legal responsibilities and for the adoption of national guidance. There is therefore a clear chain of management accountability and responsibility for Records Management and Information Lifecycle.

5.2 The following have specific responsibilities in relation to this policy:

5.3 **Chief Executive Officer** has overall responsibility for managing the development and implementation of records management procedural documents and for working with the Data Security & Information Governance (IG) Team who will provide some Records Management advice and guidance in line with their contractual obligations.

5.4 **Senior Information Risk Officer (SIRO)**, under delegated authority from the Chief Executive Officer will oversee compliance with the GDPR and Data Protection Act (DPA) and the development of appropriate policy and procedure. The SIRO will be advised by supported by the Data Security & IG Team. The SIRO is responsible for ensuring any suspected breach is investigated and appropriate actions taken, for managing information risk and for guaranteeing the ICB Board is adequately briefed on information risk issues.

5.5 **Data Protection Officer (DPO)** The DPO's role is to inform and advise the ICB and its staff about their obligations to comply with the GDPR and other data protection laws. They are required to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; identify training for staff and conduct internal audits. In addition, they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

5.6 **Caldicott Guardian (CG)** has responsibility for reflecting patients' interests regarding the use of patient information and is the conscience of the organisation. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner regardless of the format the information is in.

5.7 **Information Asset Owners (IAOs) / Administrators (IAAs)** under the responsibility of the SIRO will:

- be identified, provided with sufficient training material / guidance documentation to enable them to carry out the role and will carry out risk assessments on the information assets, to protect against unauthorised access or disclosure, within their area;
- ensure the integrity of the information within their area and restrict the use to only authorised users who require the access;

- be responsible for the Information Asset assigned to them;
- ensure that all personal data can at all times be obtained promptly from the Information Asset when required to process a Subject Access Request;
- ensure that personal data held in the Information Asset register is maintained in line with the ICB's Record Management Policy, specifically around maintaining the accuracy, validity and quality of the personal data. Any personal data when no longer required should be removed promptly in line with policy.

5.8 **Data Security & Information Governance Team** is responsible for the overall development and maintenance of record management practices throughout the organisation; for drawing up guidance for good records management and data quality practice, promoting compliance with this policy in such a way to ensure the easy, appropriate and timely retrieval of information.

5.9 The ICB's **Steering Group** will be responsible for ensuring that this policy and procedure is implemented and that the records management system and processes are developed, co-ordinated and monitored.

5.10 **Directors and senior managers** are accountable for the quality of records management within the ICB and all line managers must ensure that their staff, whether administrative or clinical, are adequately trained and apply the appropriate guidelines, that is, they must have an up-to-date knowledge of the laws and guidelines concerning confidentiality and data protection.

5.11 **All ICB employees** (including temporary and contract staff), whether clinical or administrative, who create, receive and use records in any form of media have records management responsibilities. All staff must ensure they keep appropriate records of their work in the ICB and manage those records in keeping with this policy and with any guidance. Furthermore, any record that any individual creates is a public record and may be subject to both legal and professional obligations, including compliance with relevant legislation included the Freedom of Information Act, the Data Protection Act and GDPR. This responsibility is established at, and defined by, the law (Public Records Act 1958).

5.11.1 Staff will receive instruction and direction regarding the policy from several sources:

- policy/strategy and procedure manuals;
- line manager;
- other communication methods (e.g. team brief/team meetings); and
- staff Intranet.

5.11.2 All staff are mandated to undertake the Data Security Awareness Programme modules via ESR. Information Governance training is required to be undertaken on an annual basis.

5.11.3 In line with the Code of Conduct, it is the responsibility of all staff to ensure that they keep appropriate records of their work in the ICB and manage those records in keeping with this policy and any guidance subsequently produced. All employees must:

- Record any important and relevant information, making sure that it is complete;
- Ensure that if written it is legible so that it can easily be read and reproduced when required;
- Retain where it can be found when needed;
- Keep it up to date;
- Only use and share information where necessary;
- Suitably dispose of records as soon as possible (see NHS Records Management Code of Practice for appropriate retention periods).

This applies to all staff including those on temporary or honorary contracts, agency staff and students.

6. Processes and Procedures

The following processes and procedures must be followed to comply with this policy:

6.1 Inventory of Records held

6.1.1 The ICB will establish and maintain mechanisms through which Directorates and other units can document the records they are maintaining. The inventory of record collections will facilitate:

- the classification of records into series; and
- the recording of the responsibility of individuals creating records.

6.1.2 The register will be reviewed annually with the support of the IG team.

6.2 Record Creation

6.2.1 The ICB should have a process for documenting its activities, taking into account the legislative and regulatory environment in which it operates.

6.2.2 Records must hold adequate ‘integrity’ so their evidential weight is legally admissible and can withstand scrutiny in the event of litigation or claim. True and accurate records protect the right of the individual or the ICB.

6.2.3 All records should be complete and accurate:

- to allow staff to undertake appropriate actions in the context of their responsibilities;

- to protect legal and other rights of the organisation, patients, staff and other people affected;
- to show proof of validity and authenticity.

6.2.4 Records should be created and maintained in a manner that ensures that they are clearly identifiable, accessible, and retrievable in order to be available when required. All records should have a unique number or filling system, which will be applicable only to that record. For example, a patient's medical record will be identifiable by the NHS number and an employee's personal file held in personnel number. Records must have clear and precise formats and must be structured in the same way that files of the same description are structured with an easy to follow standard index, either numerical, by date or alphabetically.

6.2.5 The following should be documented when a paper or electronic record is created:

- file reference;
- file title;
- if appropriate protective marking i.e. Customer Confidential/ICB Confidential;
- if possible an anticipated disposal date and what action to take;
- where action cannot be anticipated, mechanisms must be in place to ensure this action takes place when the file is closed;
- all filling systems to be documented and kept up to date.

6.2.6 Managers of departments should ensure staff are made aware of their responsibilities, are properly trained and that reviews and monitoring for compliance are undertaken.

6.2.7 All major decisions or key actions which may result from discussions or meetings should be recorded as this provides key evidence of business decision making activity.

6.2.8 The ICB will ensure consistency is established in the way information is presented to target audiences, both internally and externally. When creating a record, the ICB will need to achieve the following:

- Hold the necessary records to enable staff to perform their duties;
- Ensure information can be located promptly and time wasted on locating or recreating lost documents reduced;
- Appropriate disclosure of information to staff or the public who require and are authorised to access;
- Evidence of individual and corporate performance and activity;
- Physical and digital space is used effectively;
- Records created can meet the ICB's legal obligations;
- Organisations can preserve its corporate memory and track business decisions or transactions over time.

6.2.9 See Appendix 3 for further guidance regarding record creation.

6.3 Record Quality

6.3.1 All ICB staff should be trained in record creation use and maintenance, consummate to their roles, including understanding what should be recorded and how it should be recorded and the reasons for recording it. Staff should know:

- how to validate the information with the patient or the carer or other records to ensure they are recording the correct data;
- why they are recording it;
- how to identify, report and correct errors;
- the use of the information and record;
- what records are used for and the importance of timeliness, accuracy and completeness;
- how to update and add information from other sources.

6.3.2 Full and accurate records must possess the following three essential characteristics:

- Content – the information it contains (text, data, symbols, numeric, images or sound);
- Structure – appearance and arrangement of the content (style, font, page and paragraph breaks, links and other editorial devices).
- Context – background information that enhances understanding of the business environment/s to which the records relate (e.g. metadata, software) and the origin (e.g. address title, function or activity, organisation, program or department).

6.3.3 The structure and context of each record will alter depending on the record being created. For example, policies will need to hold contextual information like author names, review date and ratification information; whereas agenda does not require that type of information but should include attendees, venue, date and time.

6.3.4 See Appendix 4 for more information on record quality.

6.4 Quality Checking

6.4.1 The ICB should establish quality checks which will minimise/eradicate errors. A different member of staff should quality check to the one that has input the information. Dependent on the type of record the following checks should be undertaken:

- ensure the correct retention period has been input onto the document which confirms the right retention/destruction will have been calculated;
- ensure all names are spelt correctly and in the correct format;

- ensure the unique identifiers are correct and in the right format;
- check the barcode number is correct (if relevant);
- the inventory should be checked for all other possible errors.

6.5 Data Set Change Notices and Advance Notification

6.5.1 A Data Set Change Notice (DSCN) and Advance Notification (AN) is the mechanism for introducing an information requirement or information standard to which the NHS, those with whom it commissions services and its IT system suppliers, must conform.

6.6 Record Keeping

6.6.1 Implementing and maintaining an effective records management service depends on knowledge of what records are held, where they are stored, who manages them, in what format(s) they are made accessible, and their relationship to organisational functions. An information inventory or record audit is essential to meeting this requirement. The inventory will help to enhance control over the records and provide valuable data for developing records appraisal and disposal policies and procedures.

6.6.2 Paper and electronic keeping systems should contain descriptive and technical documentation to enable the system to be operated efficiently and the records held in the system to be understood. The documentation should provide an administrative context for effective management of the records.

6.6.3 All records must conform to these record keeping guidelines, legislation, NHS Resolution (NHSR), Department of Health, Information Governance requirements and professional guidelines.

6.6.4 Emergency Preparedness, Resilience and Response (EPRR) - Record Keeping

The day-to-day management of people and patients in the NHS is subject to legal obligations such as duties of care, candour and confidentiality as well as professional obligations. This does not change when responding to an incident. However, these events can lead to greater public and legal scrutiny, this may include coroners' inquests, public inquiries, criminal investigations and civil action. When planning for and responding to an incident, all decisions made, or actions taken must be recorded and stored in a way that can be retrieved later to provide evidence.

6.6.5 Emergency Preparedness, Resilience and Response (EPRR) - Logging and Records Retention

NHS-funded organisations must have appropriately trained and competent Loggists to support recording of decisions made in the management of an incident. Loggists are an integral part of any incident management team. All those tasked with logging must do so to best practice standards and understand the importance of logs in the decision-making process, evaluation and identifying lessons, and as evidence for any subsequent inquiries.

Following an incident, internal investigations, external scrutiny and/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, all decisions made, or actions taken must be recorded and stored in a way that can be retrieved later to provide evidence. It may be necessary to provide all documentation; therefore, robust and auditable systems for documentation and decision-making must be maintained.

6.7 Record Maintenance

6.7.1 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 record transactions.

6.7.2 Storage accommodation for current records should be clean and tidy, should prevent damage to the records and should provide a safe working environment for staff.

6.7.3 For records in digital format, maintenance in terms of back-up and planned migration to new platforms should be designed and scheduled to ensure continuing access to readable information.

6.7.4 Equipment used to store current records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allow maximum accessibility of the information commensurate with its frequency of use.

6.7.5 When paper records are no longer required for the conduct of current business, their placement in a designated secondary storage area may be a more economical and efficient way to store them. Procedures for handling records should take full account of the need to preserve important information and keep it confidential and secure. Archiving policies and procedures should be observed for both paper and electronic records.

6.7.6 All individual files should be weeded on a regular basis, to ensure the key documentation is readily identifiable and accessible. Bulky files should contain no more than 4 years' worth of records. Any file older than this should be culled and removed to an inactive file. The front cover of each such volume must clearly indicate that other volumes exist.

6.7.7 Any duplicate documents (except where copy letters sent or received have had comments added by hand) should be culled and confidentially destroyed.

6.7.8 In order to identify when records were last active or the service user was last in contact with the service, it is advisable that year labels are used on the front cover.

6.7.9 If there are separate sets of records relating to the same service user which is a consequence of historic practice, these should all be stored together upon discharge and kept together when archived.

6.7.10 A contingency or business continuity plan should be in place to provide protection for all types of records that are vital to the continued functioning of the organisation. Key expertise in relation to environmental hazards, assessment of risk, business continuity and other considerations is likely to rest with information security staff and their advice should be sought on these matters. An annual risk assessment shall be carried out by the Information Asset Owner to identify the security weaknesses or business continuity risk. Information Asset registers should be included in the directorate business continuity plan.

6.8 Tracking of Records

6.8.1 Accurate recording and knowledge of the whereabouts of all clinical and non-clinical records is essential if the information they contain is to be located quickly and efficiently. Records must not be taken out of the office unless this has been agreed by the Line Manager and a tracking mechanism is in place. The tracking system could be manual or electronic and linked to a department's IT system.

6.8.2 Tracking mechanisms should record the following (minimum) information:

- The item reference number of the record or other identifier;
- a description of the item (e.g. file title);
- the person, unit or department, or place to whom it is being sent;
- the date of the transfer to them;
- the date of the information returned (if applicable).

6.8.3 Manually operated tracking systems are common methods for manually tracking the movements of active records and include the use of:

- a paper register – a book, diary, or index card to record transfers, item reference number of the record or other identifier;
- file "on loan" (library type) cards for each absent file, held in alphabetical or numeric order;
- file "absence" or "tracer" cards put in place of absent files.

6.8.4 Electronically operated tracking systems include:

- a computer database, excel spread sheet in place of paper/card index;
- bar code labels and readers linked to computers;
- work flow software to electronically track documents.

6.8.5 The minimum data which needs to be recorded includes:

- service user's name;
- NHS number;
- date the records were removed;
- destination and name of intended recipient;
- name of the person releasing the records.

6.8.6 A well thought out, manual or electronic system should:

- provide an up-to-date easily accessible movement history and audit trail;
- be routinely checked and updated;
- be recorded i.e. all movements of a record even if the record is exchanged between teams / staff members within the same building;
- provide a return receipt and it made clear to whom the records should be returned;
- ensure information recorded on the tracking system must be correct and applicable to ensure the system remains effective;
- take into consideration any filing that comes in whilst the records are traced out and must be filed according to local documented procedures until such time as the records are returned;
- ensure that any records are returned safely to their correct home and absent records are chased on a frequent basis;
- maintain a log of all records received into the department including the date received, service user name and NHS number.

6.8.7 Managers should ensure that training and procedures are in place for manual and electronic tracking systems and that they are being adhered to.

6.9 Record Transportation

6.9.1 All ICB employees and contractors have a legal duty to keep information safe and secure. Security and confidentiality of records should always be paramount. This is particularly important, in high security risk situations such as the transportation of records between sites. Records should not be taken off site without the authorisation of the relevant line manager. To reduce the risk of loss of records and the risk of breaches of confidentiality, staff are advised to observe the following minimum precautions:

- Records should be tracked out of the respective department so that other staff are aware of the location of the record;
- records should never be left unattended where it would be possible for an unauthorised person to have access to them;

- records being transported should always be kept out of sight;
- if records are taken home, they must be stored securely.

6.9.2 NHS organisations are required to map their information flows in accordance with the requirements of NHS England's DSPT. The objective of this is to demonstrate that an organisation, in this case the ICB, clearly identifies and has addressed the risks associated with the transfer of identifiable information. This mapping requires all organisations to have an up to date register of information transfers (i.e. audit or mapping the flows of information in and out across the organisation). The ICB maintains an Information Sharing Register for the documenting of all uses and flows of personal information in accordance with GDPR Article 30 and DPA 18 Schedule 1 Part 4.

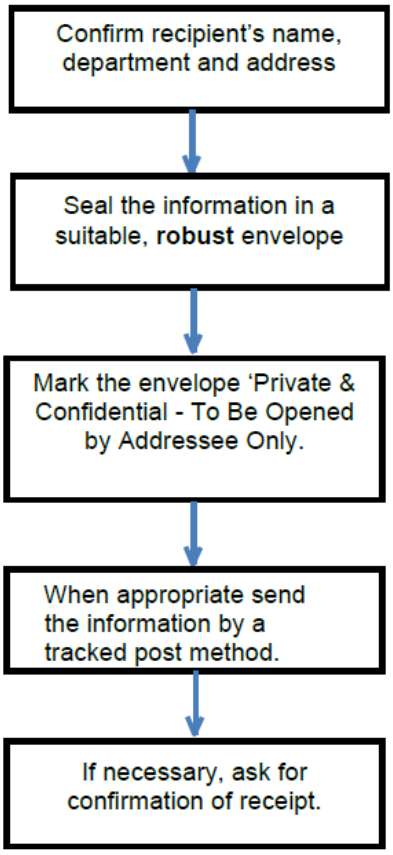
6.9.3 Security requirements also apply when staff records are transported. It is recognised that staff may find it necessary to remove records from their base, to ensure business continuity. To reduce the risk of loss of such records and to reduce the risk of breaches of confidentiality there are various considerations to be made, based on best practice:

- Records should not be removed for administrative purposes i.e. writing reports. A trace should be kept at the base from which records have been removed and staff are aware of the location of the record;
- Records should not be left unattended in cars;
- Records kept in any staff possession should remain safe and secure at all times i.e. out of sight and locked away when not in use;
- Records should only be taken off site with the approval of the Line Manager;
- Any vehicle used for the transportation of records must be insured for business use. If the staff member is involved in a road traffic accident which necessitates the car being left on the roadside or taken to a garage, records should be removed.
- If this is not possible the matter should be reported to the Line Manager and an incident form completed.
- Where external courier services are used to transfer patient health records between health organisations, a formal contract/ service level agreement needs to be put in place, which should include a confidentiality clause. A sealed package should be presented to the courier for signature, which should then be signed for by the organisation receiving the records.
- Employees must only send and ask for medical records to be transferred by recorded delivery / courier in an emergency.
- Health or social care records or other confidential information for transportation between ICB sites/departments must be enclosed in sealed bags/envelopes and labelled appropriately i.e. Confidential or Safe Haven. For specific situations of extreme sensitivity i.e. child protection, a further statement should be added stating 'to be opened by addressee only'.

- If paper health records are held that require transportation between ICB sites/departments, they must be carried by authorised staff only. Authorised staff may include:
  - Appropriate member of staff;
  - Internal transport systems;
  - Authorised courier service;
  - Off-site records storage supplier;
  - Special delivery service by Royal Mail.
- Transfer of information slips / records or an equivalent electronic process should be used to track movement of records.
- The records should not be left unattended in transit at any time. When carried in a car they must be out of sight, i.e. locked in the boot.
- Only in exceptional circumstances may records be taken home by a member of staff to work on. Staff who do so will be responsible for the security and confidentiality of the records.
- Where appropriate, use a copy.

A record must be kept for any transportation of records from one place, organisation or department to another.

6.9.4 Flowchart for sharing Personal, Confidential or Sensitive Information by Post:



6.10 Lost/Missing Records

6.10.1 A lost/missing record is a record either that cannot be found following a search in the office environment or is unavailable.

6.10.2 The loss of records constitutes a reportable incident and should be reported on the ICB's Incident Reporting System in accordance with the ICB's Incident Reporting Procedure. The line manager will be responsible for tracing the record, informing the IAO and IAA, and reporting the incident.

6.10.3 It is importance that records can be retrieved at any time during the retention period, whether for management or legal purposes.

6.10.4 See Appendix 5 for more information regarding Lost/Missing records.

6.11 Scanning

6.11.1 For reasons of business efficiency and in order to alleviate storage space/issues, the ICB can scan into electronic format inactive records which exist in paper format. The following factors should be considered:

- the initial costs of the scanning and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept;
- the need to consult in advance with the local Place of Deposit or The National Archives regarding records which may have archival value, as the value may include the format in which it was created; and
- the need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008).

6.11.2 In order to fully realise the benefits of reduced storage requirements and business efficiency, the ICB will securely dispose of the paper records that have been copied into electronic format and stored in accordance with appropriate standards.

6.12 Disclosure and Transfer of Records

6.12.1 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. Guidance should be sought from the ICB's IG Team prior to any disclosure. If the request for access to information is made under the FOI Act 2000, then the request should immediately be forwarded to the FOI Team in order to comply with the deadlines specified in the Act.

6.12.2 The ICB IG Team should be made aware of any proposed disclosure of confidential patient information, informed by the Department of Health publication Confidentiality: NHS Code of Practice.

6.12.3 The mechanisms for transferring records from one organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held. The Information Governance Team can advise on appropriate safeguards.

6.13 Retention, Archiving and Disposal of Records

6.13.1 Records appraisal refers to the process of determining whether records are worthy of additional retention or permanent archival preservation. If the latter, this should be undertaken in consultation with the National Archives, or with an approved Place of Deposit where there is an existing relationship.

6.13.2 The purpose of the process is to ensure that 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.

6.13.3 The procedure for recording the disposal decisions made following appraisal must be followed. The ICB will determine the most appropriate person(s) to carry out the appraisal in accordance with the retention schedule. This should be a senior manager with appropriate training and experience who understands the operational area to which the record relates.

6.13.4 Most NHS records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage of the lifecycle of the record, including destruction, and that the method used to destroy such records is fully effective and ensures their complete illegibility.

6.13.5 Staff leaving employment with NHS Central East ICB must ensure that they have reviewed and cleared down their OneDrive and personal NHS mail accounts of all data relating to ICB business e.g. documentation related to incidents, person/patient identifiable or business sensitive data and re-saved within a restricted sub-site within O365 (SharePoint). Leavers must complete the Leaver's Checklist in conjunction with their line manager and forward to the ICB's HR Team for retention within their personnel file. If additional guidance is required on retention/disposal of data, please contact the Information Governance.

6.14 Retention of Incident (EPRR) Records

6.14.1 In any incident, it is important that a comprehensive record is kept of all events, decisions, reasoning behind key decisions and actions taken. Each organisation is required to maintain its own records and those involved in the incident should retain all their records. For those who make decisions, it is very important to have a comprehensive and accurate log of what you have done during the incident as this represents a permanent record that could be used for internal or external inquiry at any time, often several years after the event or incident. Please refer to EPPR policy.

6.15 Record Closure

6.15.1 Records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes. Each year a list of records coming to the end of their retention period should be reviewed. An indication that a file of paper records or folder of electronic records has been closed, together with the date of closure, should be shown on the record itself as well as noted in the index or database of the files/folders. Where possible, information on the intended disposal of electronic records should be included in the metadata when the record is created.

6.15.2 Records/information contain personal confidential information and it is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy records is fully effective and complete illegibility is secured. Destruction of all records, regardless of the media in which they are held should be conducted in a secure manner ensuring safeguards are in place against accidental loss or disclosure.

6.16 Retention Schedules and Record Disposal

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

6.16.2 The ICB has adopted NHS England's retention periods set out in the Records Management: Code of Practice. These retention schedules outline the recommended minimum retention period for NHS records.

6.16.3 Senior Managers will be responsible for ensuring disposal schedules are implemented as part of a rolling programme. Recommended minimum retention periods should be calculated from the end of the calendar year following the last entry to the document. i.e. a file's first entry is in February 2001 and the last December 2006, the minimum retention period is eight years, it should therefore be kept in its entirety at least until 31st December 2014. If a member of staff feels that a particular record needs to be kept for longer than the recommended minimum period or there is a specific purpose further advice and approval should be sought from the Service Senior Manager or Director.

6.16.4 Records selected for archival preservation and no longer in regular use by the organisation should be transferred as soon as possible to an archival institution that has

adequate storage and access facilities. Non-active records should be transferred no later than 30 years from creation of the record, as required by the Public Records Act.

6.16.5 The Public Records Act requires certain public bodies to transfer records of historical value for permanent preservation to local archive services appointed as 'places of deposit' (PoD). The point of transfer was by the time the records reached 30 years old. Changes in legislation mean that since 1 January 2015 specified local public sector organisations (magistrates' courts, prisons, coroners' courts, NHS bodies and some arms-length bodies including the Environment Agency) must now transfer records selected for permanent preservation to a place of deposit at 20 years after their creation, rather than the previous 30 years. Transferred records should be in good condition and appropriately packed, listed and reviewed for any FOIA exemptions. More detailed guidance on the selection for records for transfer under the Public Records Act 1958 can be found on The National Archives website.

6.16.6 The relevant PoD will provide additional local guidance on how the schedules should be implemented. As a general rule, national public sector organisations will deposit with The National Archives while local organisations will deposit with a local PoD.

6.16.7 Records over 30 years old and selected for permanent preservation must be transferred to the Public Record Office or kept in a 'relevant place of deposit' for public records. In most cases, such records will be stored in the nearest Local Authority Record Office.

6.16.8 Records not selected for archival preservation and which have reached the end of their administrative life should be destroyed in as secure a manner as is appropriate to the level of confidentiality or protective markings they bear.

6.16.9 The methods used throughout the destruction process must provide adequate safeguards against the accidental loss or disclosure of the contents of the records. Contractors, if used, are required to sign confidentiality undertakings and to produce written certification as proof of destruction.

6.16.10 A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the ICB.

6.16.11 If a record due for destruction is the subject of a statutory request for information or potential legal action, destruction should be delayed until disclosure has taken place or the legal process complete. Advice should be obtained from the Information Governance Lead.

6.16.12 It must be remembered that the destruction of records is an irreversible act.

6.17 Classification of documents (for FOI purposes)

6.17.1 When classifying NHS documents regard should be paid to the requirements of the Freedom of Information Act 2000.

6.17.2 Consideration should be given before marking documents that would normally be published or disclosed on request. Over-classification might lead to inappropriate decisions not to disclose information that would later be embarrassing to the ICB.

6.17.3 Protective markings should wherever possible be restricted to information that would be exempt from disclosure, including temporary exemptions, such as the drafts of documents that are intended for publication.

6.17.4 On receipt of Freedom of Information requests staff should forward onto the ICB FOI mailbox for management of response.

6.18 Information Requests – Access to Health Records (AtHR) and Subject Access Request (SAR)

6.18.1 A Subject Access Request, commonly referred to as a SAR, is a request from a data subject to see a copy of personal information that is held about them by an organisation. All data subjects have the right (subject to exemptions) to access personal information which is kept about them by the ICB, both in electronic and paper files. See Right of Access Information Commissioner's Office (ICO).

6.18.2 Any individual is entitled to:

- Know what information is held about them and why;
- Gain access to it regardless of the media which it is held;
- Have their information kept up to date;
- In some situations, require the ICB to rectify/block, erase or destroy inaccurate information;
- Not have confidential information processed about them likely to cause damage or distress;
- Not have confidential information processed about them for the purposes of direct marketing.

6.18.3 In certain cases, the ICB will only process personal information with the consent of the data subject. If the information is sensitive, explicit consent may be needed. It may be a condition of patients, and employment of staff, that they have been made aware and agree to the ICB processing specific classes of personal information.

6.18.4 The ICB may sometimes process information that by this definition is classed as sensitive. Such information may be needed to ensure safety, or to comply with the requirements of other legislation.

6.18.5 The Access to Health Records Act 1990 provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements.

For further guidance and information please see the ICB's Request for Information Policy which incorporates SARs.

6.19 Records Management and System Audit

6.19.1 The process for monitoring and evaluating the effectiveness of this policy, including obtaining evidence of compliance will be part of the ICB's Data Security and Protection Toolkit annual self-assessment.

6.19.2 The ICB will audit its records management practices for compliance with the framework to:

- identify areas of operation that are covered by the ICB policies and identify which procedures and/or guidance should comply to the policy;
- follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance: and
- highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment related procedures.

6.19.3 The results of audits will be reported to the ICB IG Steering Group and exceptions escalated to the ICB Audit & Risk Committee.

6.20 Training and Awareness

6.20.1 ICB staff are mandated to undertake Information Governance training (in the form of Data Security Awareness e-Learning module) annually. Good Record Keeping features within this training. All ICB Staff will be made aware of their responsibilities for record-keeping and record management.

6.20.2 Where staff may take on a specific Information Governance role within the ICB e.g. Records Management, dealing with Access to Records, Data Protection Impact Assessments or Information Asset Ownership, additional Information Governance training may be required.

6.20.3 The IG Training (Data Security Awareness e-Learning module) will be utilised, and uptake will be monitored. Where required for specific teams the ICB will deliver annual face to face training sessions that include Records Management.

6.20.4 The ICB IG Steering Group will be responsible for ensuring that this policy and supporting procedures are implemented, and that the records management system and processes are developed, co-ordinated and monitored.

6.20.5 This policy and procedure will be promoted and placed on the ICB's website for all staff to access.

6.20.6 To maintain high staff awareness, the ICB will direct staff to several sources:

- policy/strategy and procedure manuals;
- line manager;
- specific training courses;
- other communication methods, for example, team meetings; and staff extranet.

7. Statutory and National Guidance

7.1 This policy has been developed with reference to the following statutory and national guidance:

- The Public Records Act 1958 and 1967;
- The Data Protection Act 2018/General Data Protection Regulation (GDPR);
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice; and
- National Archive - http://www.nationalarchives.gov.uk/
- Records Management Code of Practice - NHS Transformation Directorate

7.2 All NHS records are public records under the Public Records Acts. The ICB will take actions as necessary to comply with the legal and professional obligations set out in the NHS Records Management Code of Practice and any new legislation affecting records management as it arises.

7.3 The ICB will also take action to comply with any new legislation affecting records management as it arises.

7.4 Under the FOI Act 2000, once a record has been requested, it cannot be destroyed. It is a criminal offence to amend, erase or destroy information once a request is received.

8. Stakeholder Engagement Record

8.1 The following stakeholders were engaged in the development this policy:

Role/Group	Date of Engagement	Summary of Feedback
Joint IG Steering Group	6th March 2026	Changes made, ready for Board Approval.
CEICB Board	1st April 2026	TBC

Accessibility Statement

This policy is available in alternative formats upon request, including large print, Braille and translated versions, to ensure accessibility for all staff and stakeholders.

Implementation Plan

Development and Consultation: The following individuals were consulted and involved in the development of this document:

- Information Governance Team
- Joint IG Steering Group

Dissemination: Staff can access this document via the staff website and will be notified of new/revised version via the internal staff newsletter.

Training: The following training will be provided to make sure compliance with this document is understood:

- All new staff are required to attend a compulsory Induction Programme which incorporates Information Governance.
- In addition to this, all staff are required to complete and pass the NHS Data Security Awareness training on an annual basis.

Monitoring: Monitoring and compliance of this document will be carried out via:

- An assessment of compliance regarding information sharing is undertaken within the Data Security and Protection Toolkit, each year and audited by internal auditors.
- In addition, the ICB's Data Security & IG Team will undertake additional monitoring of compliance with this policy as a response to identification of any gaps or as a result of risks identified by incidents, external reviews or other sources of information and advice.

Review: The Document Owner will ensure this document is reviewed in accordance with the review date.

Equality, Diversity, and Privacy: See Appendices

Associated Documents: The following documents must be read in conjunction with this document:

- Information Sharing Policy
- Information Governance Framework Policy
- Access to Records Policy
- Data Protection Policy
- ICB Privacy Notice
- EPRR Policy

NHS
Central East
Integrated Care Board

Appendix 1: Equality Impact Assessment

Please answer the questions against each of the protected characteristic and inclusion health groups. If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken. It is against the law to discriminate against someone because of these protected characteristics. For support and advice on undertaking EQIAs please contact: agcsu.equalities@nhs.net

Name of Policy:	CEICB Records Management & Lifecycle Policy
Date of assessment:	February 2026
Screening undertaken by:	Data Security & IG Officer

Protected characteristic and inclusion health groups. **Find out more about the Equality Act 2010, which provides the legal framework to tackle disadvantage and discrimination:** **https://www.equalityhumanrights.com/en/equality-act/protected-characteristics**	**Could the policy create a disadvantage for some groups in application or access?** **(Give brief summary)**	**If Yes - are there any mechanisms already in place to mitigate the potential adverse impacts identified?** **If not, please detail additional actions that could help.** **If this is not possible, please explain why**
Age A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).	No	
Disability A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.	No	
Gender reassignment The process of transitioning from one gender to another.	No	
Marriage and civil partnership	No	

Marriage is a union between a man and a woman or between a same-sex couple. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.		
Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.	No	
Race Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour and nationality (including citizenship) ethnic or national origins.	No	
Religion or belief Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.	No	
Sex A man or a woman.	No	
Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none.	No	
Carers Individuals within the ICB which may have carer responsibilities.	No	

Please summarise the improvements which this policy offers compared to the previous version or position.
N/A
Has potential disadvantage for some groups been identified which require mitigation?
No – (If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken.)

NHS
Central East
Integrated Care Board

Appendix 2: Data Protection Impact Assessment

Screening questions to determine if a full DPIA is required. Guidance on handling personal and sensitive data.

Data protection is the fair and proper use of information about people. Before completing this form, please refer to the Data Protection Impact Assessment (DPIA) Guidance in the Information Governance (IG) section on the staff Intranet or contact the Data Protection Officer for support via ***(insert email address once confirmed)***

A DPIA is a process to help you identify and minimise the data protection risks. You must do a DPIA for processing that is likely to result in a high risk to individuals. You can use our screening checklist below to help you decide when to do one. If you have answered 'Yes' to any of the 10 screening questions, you must then carry out a full DPIA using the Stage 2 form, which is also available on the Intranet in the IG section.

Name of Policy:	CEICB Records Management & Lifecycle Policy
Date of assessment:	February 2026
Screening undertaken by:	Data Security & IG Officer

Stage 1 – DPIA form **please answer 'Yes' or 'No'**

1. Will the policy result in the processing of personal identifiable information / data? This includes information about living or deceased individuals, including their name, address postcode, email address, telephone number, payroll number etc.	Yes
2. Will the policy result in the processing of sensitive information / data? This includes for living or deceased individuals, including their physical health, mental health, sexuality, sexual orientation, religious belief, National Insurance No., political interest etc.	Yes
3. Will the policy involve the sharing of identifiers which are unique to an individual or household? e.g., Hospital Number, NHS Number, National Insurance Number, Payroll Number etc.	Yes
4. Will the policy result in the processing of pseudonymised information by organisations who have the key / ability to reidentify the information? **Pseudonymised data -** where all identifiers have been removed and replaced with alternative identifiers that do not identify any individual. Re-identification can only be achieved with knowledge of the re-identification key. **Anonymised data -** data where all identifiers have been removed and data left does not identify any patients. Re-identification is remotely possible, but very unlikely.	Yes
5. Will the policy result in organisations or people having access to information they do not currently have access to?	No
6. Will the policy result in an organisation using information it already holds or has access to, but for a different purpose?	No
7. Does the policy result in the use of technology which might be perceived as being privacy intruding? e.g., biometrics, facial recognition, CCTV, audio recording etc.	No

8.	**Will the policy result in decisions being made or action being taken against individuals in ways which could have a significant impact on them?** Including profiling and automated decision making. (This is automated processing of personal data to evaluate certain things about an individual i.e., diagnosis and then making a decision solely by automated means - without any human involvement)	No
9.	**Will the policy result in the collection of additional information about individuals in addition to what is already collected / held?**	No
10.	**Will the policy require individuals to be contacted in ways which they may not be aware of and may find intrusive?** e.g., personal email, text message etc.	No

Appendix 3: Creating a Record Checklist

Check you know how to create adequate records and what information they should contain;

- Follow relevant ICB policies and guidelines to ensure creating full and accurate records;
- Establish and document local procedures on creating business critical records to the department, or if using a corporate or local proforma; and ensure procedures are followed;
- Use corporate templates wherever available so it clearly identifies the nature of the information and type of document;
- Include fundamental elements like author, date, title, department, contact details, and holds the approved corporate identity;
- Ensure documents hold the relevant information specifically required for that type of record, like in the case of policies or forms. In the example of a policy this would include: executive signature, approval route, review date;
- Capture decision-making in minutes or when creating records or emails, and that you maintain a record of any transactions. For example, agreements or discussions that impact on your work or with other teams/organisations;
- Always ensure that the information you are recording is accurate and objective;
- Use standard terms to describe documents and be consistent with use of acronyms;
- Identify the creator and use their job title, plus other people who may have contributed to the document;
- Explain within the text of the document, any codes or abbreviations used, as their meaning may become less clear over time;
- Do not use logos, icons or catchphrases on documents that have been formally approved; include the ICB logo in all appropriate records;
- Remember that your records, or local record keeping practises may be required for performance checks or in the event of a claim or litigation.

Appendix 4: Quality of Record Entries

Good record keeping is a mark of skilled and safe practice, whilst careless or incomplete record keeping often highlights wider problems with individual practice.

Examples of good record keeping below:

- Structure and Content of Records;
- Where possible there must be one set of records for each data subject/individual;
- Unique Identifier;
- A unique identifier must be used to ensure that records can be retrieved when archived or stored.

Record entries should be:

- Complete, factual, consistent and accurate
- Legible, clear and unambiguous
- Contemporaneous, i.e. written as soon as possible
- Consecutive and dated (and timed if appropriate)
- If appropriate, signed by the data subject/individual according to the service specific policies
- Only in exceptional circumstances, should entries to records be delayed
- Not include abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subjective statements
- Be written clearly and in such a manner that the text cannot be erased.

Abbreviations

Abbreviations must not be used routinely.

Alterations

Contemporaneous alterations to records are acceptable when an entry has been made in error.

When this occurs, the author must take the following actions:

- Make an entry stating “written in error” near the incorrect entry
- Sign, date and record the time of the annotation making the change
- Strike through the original entry with a single line leaving it discernible
- Make the correct entry, signing it and dating it.

It is unacceptable to:

- Delete or erase notes, such that the entry is no longer legible
- Use correction fluids of any part of a clinical record
- Change original entries, other than as specified above
- Change entries made by another person.

Appendix 5: Procedure for handling Missing/Lost records

Lost records

- The member of staff should report the missing record to his/her supervisor/ manager as soon as possible;
- The supervisor/manager should ensure that a thorough search takes place, using tracking methods, including initiating a search at the base where the record should be kept;
- The event must be reported on the ICB Incident Reporting System to alert the Data Security & Information Governance Team;
- A temporary record should be created, clearly marked as a temporary record, populated with all relevant information available for that data subject/individual. A temporary record should be set up and tracked on the relevant systems for the Department;
- When original records are located the missing record log should be updated with details of where/how the original was located, and the two folders should be merged.

Unavailable/Missing records

- A record is regarded as unavailable if it is in use elsewhere and/or cannot be retrieved in time for an appointment;
- Any unavailable/missing records must be reported on the ICB Incident Reporting System to alert the Data Security & Information Governance Team;
- A temporary record should be created, as described in the above section
- If an appointment is deferred (i.e. individual has a meeting/appointment with HR) as the record is not available this should also be reported.

Reasons for records being unavailable may include:

- Record needed for another appointment/meeting
- Record with another Team/ Department
- Record not tracked
- Misfiled
- Wrong record/volume/temp record(s) sent

Appendix 6: Disposal of Unwanted Equipment and Information

Introduction

It is vital that confidentiality is safeguarded at disposal. Therefore, it is all employees' responsibility to ensure that the chosen method used to destroy records is fully effective and secures their complete illegibility. Methods may include: Shredding, Pulping, Incineration.

All information about people and the organisation should be disposed of in a secure manner when no longer required regardless of the media on which it may be held.

Prior to disposing of any information, employees should consult NHS Central East ICB's Records Management and Lifecycle Policy in conjunction with the NHS Records Management Code of Practice, to ensure that it is legal to dispose of the information. These policies outline the retention periods for information, and covers employee records, administrative records, estates records, reports, investigations and complaints etc. All relevant policies are available on the ICB's website.

All employees will be informed of the correct methods of disposal of waste/ unwanted information through staff training, induction and/or making them aware of policies and guidance available on the website.

Destruction of paper waste

It is important that all paper type business waste material is disposed of in a secure manner, to maintain confidentiality and comply with legal requirements.

All waste/unwanted paper will be disposed of by placing in the paper recycling bins or locked confidential blue bins located in:

Unwanted paper may include draft documents, unwanted agendas and minutes of meetings, any papers in files the ICB no longer needs to retain, bad photocopies or handwritten notes etc. Any papers put into the cardboard recycle bins or general rubbish bins can be extracted by anyone who wishes to see and/or use the information. Care must be taken to ensure that confidential material is identified and removed so that only general papers are disposed of in these types of bins.

Any papers that identify staff or patients or contain business sensitive information, financial information, complaints, Serious Untoward Incidents, and/or any information that may identify a patient **MUST** be put into the confidential disposal containers.

Note: If a document needs to be retrieved from the confidential waste, please contact the Data Security & IG Team.

If the information is deemed to be highly sensitive or confidential it may be necessary to shred or tear into very small pieces prior to being placed in the confidential bin.

Once the bins are full, a designated authorised contractor will collect them. The contractor will dispose of the papers in a secure confidential manner as stipulated the contractual agreement between Central East ICB and current waste provider.

Staff are reminded that they have a personal duty to ensure papers containing sensitive detail are not to be put into the ordinary waste-paper bins, as doing so will constitute a confidentiality breach.

Media	How to dispose
PAPER (non-confidential)	Put into recycling bins located in each department. The bins will be collected/emptied when full by the authorised contractor and taken away in a secure manner for pulping/re-cycling.
PAPER (confidential)	If the information is sensitive the paper must be put into one of the confidential waste containers. There is a 'post box' size opening for papers to be 'posted'. These confidential waste bins are routinely collected by the data shredder contractor who will then shred the paper securely.

Computer media

Computer media will include all the items listed in the table below. This is not an exhaustive list of all possible media as technology will evolve and new media will become available as time progresses.

If you identify anything that needs to be disposed of, please contact the HBL ICT service desk.

Below are the most common types of media in use at the time this policy was produced. This Policy will be updated regularly and therefore take account of new media throughout the review period.

Media	How to dispose

FLOPPY DISKS / **DVDs/ CDs**	The ICB do not routinely create Floppy disks, DVD, CDs but prior to disposal they must be re-initialised / reformatted and destroyed, or if defective, be physically destroyed, ideally by shredding or incineration. Once information has been removed from the disc it can be reused (only if encrypted) or, if no longer required, should be destroyed. The ICB have an agreement via an HBL supported service for the secure destruction of such items. If a staff member has such a device for destruction, please contact the HBL service desk and log your call. Prior to destruction this material should be physically locked away.
MAGNETIC TAPES	Must be re-initialised / degaussing and destroyed by incineration and/or shredding, or, if defective, will be physically destroyed by incineration. The ICB has an agreement via an HBL supported service for the secure destruction of such items. If a staff member has such a device for destruction, please contact the HBL service desk and log your call. Prior to destruction this material should be physically locked away.

PCs	Hard disc will be wiped clean (erased) and then disposed of by an HBL supported service in a secure manner as agreed with the ICB.
TERMINALS / PCs	Will be disposed of by an HBL supported service in the agreed manner. NHS Central East ICB employees will need to contact the Senior IT Manager for this process to be initiated.
LAPTOPS	Will be returned to ICT department / line manager when an employee leaves or no longer requires a laptop. The asset register must be updated to reflect change of ownership. Any information not removed by the last user will be erased prior to being re-allocated to another user. When the laptop no longer works and is beyond repair, if possible, all software and data will be removed prior to being sent to an HBL supported service for safe destruction/disposal to comply with EU requirements. This disposal is coordinated through the ICB ICT team.

LARGER HARDWARE	Will be disposed of securely and safely by an HBL supported service as detailed in the Service Level Agreement.
SOFTWARE	Will be disposed of in a secure manner when no longer required. Most software is either downloaded or if uploaded from a CD and the CDs will be disposed of as stated above.
MEMORY STICKS/ FLASH CARDS	NHS Central East ICB staff should only use ICB supplied encrypted memory sticks. When the information is no longer required, the user should delete it from the memory stick. When an employee leaves or no longer requires a memory stick it should be returned to the Senior IT Manager and not passed to another member of staff without prior agreement. However, at times other organisations may supply such devices which will need to be disposed of. Disposal can be arranged via the Senior IT Manager and the device must be kept securely until disposal is arranged.
MOBILE PHONES/ SMART PHONES	Will be returned to line manager before sending to ICB ICT Team (supported by 360com), where the phone will be re-set to the factory settings and it will be re-issued. If the phone is faulty it will be disposed of securely.
SIM CARDS/ MEMORY STICKS	If the SIM and/or memory card is faulty it will be cut into pieces and disposed of in a secure manner.
MULTI-FUNCTIONAL DEVICE / PRINTER HARDDRIVES	When a multi-functional device (MFD) / printer that contains a hard drive is removed, the hard drive should be destroyed on site or securely wiped. The company providing these devices will do so if they are informed of the requirement before they arrive to move or replace the MFD or printer. Further advice is available from the Senior IT Manager.