This document is uncontrolled once printed

Please check on NHS South East London Integrated Care Board's Intranet site for the most up to date version

NHS South East London Integrated Care Board

Information Management Policy (CG16)

V1.0

Approved by	SEL Transition Board
Date approved	22 June 2022
Name and title of originator/author	Simon Beard, AD Corporate Operations
Name and title of sponsor	Tosca Fairchild, Chief of Staff
Review date	June 2024
Description	Information Management policy for SEL ICB
Target audience	All Staff of NHS South East London (including members of the Unitary Board), Integrated Care Partnership, contractors and bidders

Version Control

Version number	1.0
Supersedes	n/a

Document Review Control Information

Version	**Date**	**Reviewer Name(s) and Job title**	**Change/amendment**

Contents

1. Introduction

1.1 This policy sets out the intentions of NHS South East London Integrated Care Board (hereafter referred to as 'SEL ICB') to manage all the information within its remit to the standards required by law and regulations. In doing so, it supports high quality commissioning and healthcare through accurate, accessible and appropriately governed information. SEL ICB has put this policy in place to ensure members of staff are fully aware of their information management responsibilities.

1.2 This document uses definitions provided by the Cabinet Office. The Cabinet Office defines data as *'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation'* and information as *'output of some process that summarises interprets or otherwise represents data to convey meaning'.* All reference to information in this document encompasses information and data. This includes information that is personal, financial or falls within any other category.

1.3 Information is a corporate asset and as such, is an important source of administrative, financial, legal, evidential, and historical information, it is vital to the organisation's future operations, for the purposes of accountability and for an awareness and understanding of its history. Information is the corporate memory of the organisation.

Information supports the formulation of policy, managerial decision-making, protects the interests of the organisation and the rights of individuals (including staff). Information supports consistency, continuity, efficiency and productivity and helps deliver services in reliable and equitable ways. It is important to ensure information and records are:

- Available when needed so that events or activities can be followed through and reconstructed as necessary;
- Accessible, located and displayed in a way consistent with their initial use, with the original or current version being identified where multiple versions exist;
- Able to be interpreted and set in context: who created or added to the record and when, during which business process, and how the record is related to other records;
- Trustworthy and hold integrity, reliably recording the information that was used in, or created by, the business process;
- Maintained over time, irrespective of any changes of format so that they are available, accessible, able to be interpreted and trustworthy;
- Secure from unauthorised or inadvertent alteration or erasure, with access and disclosure being properly controlled with audit trails tracking use and changes;
- Held in a robust format, which remains readable for as long as the information is required;
- Retained and disposed of appropriately using documented retention and disposal procedures, which include provision for retrieving and permanently preserving records with particular archival value.

SEL ICB is committed to ensuring that information, in whatever its context, is processed as determined by prevailing law and best practice. Compliance with all organisational policies is a condition of employment. A breach of policy may result in disciplinary action.

1.4 This policy outlines the legal, regulatory and best practice information framework that SEL ICB works to and the methods used to deliver and maintain this policy. This policy and commitment extends to the services SEL ICB are commissioned to provide, ensuring the appropriate use and control of information to deliver high quality healthcare to support patients and the organisation.

1.5 Where SEL ICB creates an official "record", it is expected that staff follow the Records Management: NHS Code of Practice published by the Department of Health, which is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. The Code of Practice is based on current legal requirements and professional best practice.

The Records Management Code of Practice states that *'information and records are the corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations'*. Consequently, it requires all NHS bodies to adopt a systematic and planned approach to the management of information and the determination of where a record has been created, from the moment the need for information is identified to when a record is created, through the information life cycle (creation to destruction).

1.6 SEL ICB recognises that effective information management is fundamental to good administration and operational effectiveness and is an enabler to the achievement of its strategic objectives.

2. Scope and objectives

2.1 This policy applies to all information (paper, electronic or in other formats) that is received, created, or held in the course of SEL ICB's business or in the pursuance of delivering patient care services. It must be adhered to by all permanent, contract, interim and temporary staff and any organisation or body acting as agents or on behalf of SEL ICB.

2.2 SEL ICB is committed to ongoing improvement of its information management systems, as it believes that it will gain a number of organisational benefits from doing so. These include:

- Using cloud-based technologies to make better use of, and reduce the need for physical server space;
- Provide a paperless and clear desk environment (see the policy statement below), where paper records are held by exception, out of sight and locked away when not in use, with a justification for holding hard copies of documents;
- Better use of staff time;
- Improved control of valuable information resources;
- Compliance with legislation and standards; and
- Reduced costs.

2.3 The key objectives of this policy and supporting guidance are to:

- Facilitate and effectively record all SEL ICB's operations, business and policy decisions;

- Ensure implementation of best practice in information management and record-keeping, including operating a clear desk policy and corporate file path naming convention (see below);
- Demonstrate compliance with relevant legislation;
- Raise the minimum standard of records management practice in SEL ICB to the specified standard in the Data Security and Protection Toolkit;
- Ensure that records are protected, complete, accessed and managed in line with information classification and handling arrangements;
- Ensure official records of historical and evidential significance are identified and held securely; and
- Define clear responsibilities for managers and staff.

3. Responsibilities

3.1 Information governance responsibilities are outlined within the accountability and governance section within the Information Governance Framework.

4. Information Management

SEL ICB utilises four main principles in the management of information:

Principle 1

SEL ICB will create, capture, use, manage, store and destroy or preserve its records in accordance with all statutory, business and historical requirements. It will ensure that the appropriate technical, organisational and human resource elements exist to make this possible. The primary location for SEL ICB's information will be Microsoft Office 365, a cloud-based solution.

Principle 2

Information will be created once, stored in one place and will be accessible in a timely fashion to those who need to use the information across the organisation and externally to stakeholders. This will take into account the need for effective security and appropriate confidentiality.

Principle 3

Information management will be embedded within operational procedures and activities. All staff that create, use, manage or dispose of information have a duty to protect the information and ensure that any information that they add is accurate, complete and necessary. This includes identifying where an official record is created, as defined in Annex A.

Principle 4

The risk to effective information management will be assessed corporately and managed appropriately at strategic and operational levels. Compliance with this policy and associated procedures will be subject to a programme of audit and assurance.

5. Legislative and regulatory environment

All NHS official records are public records under the Public Records Act 1958. SEL ICB will take action as necessary to comply with all legal and professional obligations in particular those contained in:

Legislation

- The Public Records Act 1958;
- Data Protection Act (2018);
- The common law duty of confidentiality;
- Human Rights Act 1998;
- Freedom of Information Act 2000;
- The Protections of Freedoms Act 2012;
- The Re-use of Public Sector Information Regulations;
- UK General Data Protection Regulation;
- Environmental Information Regulations 2004;
- NHS Act 2006;
- Health and Social Care Act 2012;
- Care Act 2014.

Best Practice Standards

- ISO 15489 - Records Management Standard;
- ISO 27001 – Information Security Standard;
- Department of Health Records Management NHS Code of Practice;
- Department of Health Records Management Roadmap;
- Confidentiality NHS Code of Practice;
- Information Security NHS Code of Practice;
- Lord Chancellor's Code of Practice on the Management of Records Issued under (s.46) of the Freedom of Information Act;
- The National Archive: Essential Records Management; and
- NHS Digital Data Security and Protection Toolkit

6. Information Asset Register

SEL ICB will establish an inventory of information. The inventory of information will facilitate:

- The classification of information into series; and
- The identification of information asset owners and administrators.

All records created by SEL ICB will follow national guidance on protective marking; see Annex B - Classification Marking of NHS Information.

7. Electronic filing structure

Electronic information held by SEL ICB will be maintained in Microsoft Office 365, a cloud-based solution hosted in the United Kingdom, which follows the principles of functions, activities and transactions of SEL ICB and matches the organisational structure. Some teams within SEL ICB will access applications hosted within local datacentres or alternative third-party IT system repositories. SEL ICT support the management and access controls of the IT network and designated repositories which provides authorised role-based access and robust security measures to protect the ICBs information.

Microsoft Office 365 has permissions to enable cross-borough and directorate working. The responsible owner of each directorate area on SharePoint is the Director responsible for the service who is also the information asset owner for that function. Associate/Assistant Directors will have operational responsibility for the management of the information within their department and/or associated team.

Authorisation for access to each team/department SharePoint library will be managed via the Directorate lead and the permission function carried out by the Office 365 ICT Service Desk through authorised role-based access form.

The name applied to any file must reflect the file content in terms of the SEL ICB function, activity or transaction it applies to (in line with the file naming convention set out in the records management policy) but must not replicate any tags already applied in the name of the file, i.e. date, name/initials of the author, version number or the tags you are prompted to add before it is uploaded.

8. Paper Filing Structure

By exception, where paper information is held, with a justification for holding hard copies of documents; records held by SEL ICB will be maintained in a file structure that follows the principles of functions, activities and transactions of the ICB. This will match the organisational and the electronic file structure, which staff in the department can easily navigate to locate files quickly. Where requests for archiving of hard copy records with our external storage provider are made this must only be for records which meet the necessary retention criteria and requests must be made following the appropriate process.

9. Record Disposal and Archiving

Disposal is defined as '*the decision on the management intent for a record once it is no longer required for the conduct of current business'.*

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

SEL ICB will adhere to the retention schedules aligned to the Records Management: NHS Code of Practice.

Disposal schedules will be the subject of regular review to identify any exceptions SEL ICB wishes to make to the national standard retention periods, subject to justification and approval by the Information Governance Sub-Committee and ratification by the Board.

Archiving is defined as *'paper or electronic records, when they are no longer required to be retained either as active or semi active records within normal working locations, but are not allowed to be destroyed'.*

SEL ICB will ensure it has an appropriate and secure location for the storage of records that have an adequate process for retrieval.

The decision to archive an official record must meet the above definition and be approved by the Information Asset Owner of the service requesting to archive records.

A review of documents for archiving should take place on an annual basis for each service.

10. Monitoring and Compliance

This policy and the associated controls will be monitored through the risk management system for SEL ICB. The risk register will be reviewed on a monthly basis and additionally in response to any information incident or enforcement action by the Information Commissioner's Office. Information risk management is a key component of wider assurance and control in setting the priorities for the information governance work plan.

Control Audit and Monitoring Table	
Monitoring requirements: What in this document is monitored?	The management of information risks. Compliance with the law. Compliance with the Data Security and Protection Toolkit. Incidents related to the breach of this policy.
Monitoring Method	Information risks will be monitored through the risk register management system. Compliance with law will be monitored through audit, work directed by the Data Security and Protection Toolkit and as directed by information risk management policy. The Data Security and Protection Toolkit will be monitored by assessment of evidence against the objective of the relevant requirement. In addition, the toolkit will be audited by the organisation's internal audit function before the annual submission. Incident reporting and management requirements.
Monitoring prepared by	Information Governance Team and Information Governance Sub-Committee Incident reports will be produced by the nominated investigation officer.
Monitoring presented to	Information Governance Sub-Committee Senior Information Risk Owner (SIRO) Caldicott Guardian (CG)
Frequency of Review	Bi-monthly updates will be provided to the SIRO and the CG or more frequently where required. Relevant information risks will be added to the corporate risk register and reported in line with the risk management system. Annual (as a minimum) updates to the Board will be provided, including the internal audit report on DSPT performance. Incident reports will be reviewed at every meeting of the Information Governance Sub-Committee and escalated to the Board as appropriate.

Further monitoring will be undertaken through the change control process.

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures may result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance they are individually responsible for. Failure to maintain these standards can result in criminal proceedings against the individual.

11. Review

Review will take place every two years or earlier until the policy is rescinded or superseded, due to legal or national policy changes.

Appendix A: Definitions

Records Management - as defined by ISO 15489

'The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records'.

Record - For the purposes of this policy the definition of a record used by SEL ICB is:

Documentary evidence, regardless of form or medium, created, received, maintained and used by SEL ICB in pursuance of its legal obligations or in the transaction of business.

This definition draws a distinction between a record and a document – a record is a final version that may be retained, while a document can be changed and will not normally be retained except for audit trail purposes where necessary. The purpose of a record is to preserve information in a form that is trustworthy and, once declared, should not be changed.

Personal Confidential Data (PCD):

E.g. patients' clinical records, patient confidential data, and information about NHS staff that passes between NHS staff, and between NHS staff and staff of other appropriate agencies. This includes patient demographic details that might identify people who have had a GP contact/hospital appointment within a particular timeframe or who may have a particular condition.

Information Lifecycle

System Design

One of the key elements of information management throughout the lifecycle of information is the design of systems to capture information and records, It is important that the procurement, commissioning or system design process completes a thorough analysis, including a data protection impact assessment.

Creation

Information when created must be authentic, accurate, accessible, complete, compliant, effective and secure and its integrity must be protected over time.

At the point of creation, the relevant metadata (breakdown details of the data) needs to be captured to ensure its on-going value and evidential weight.

Use

All information must be used consistently, only for the intentions for which it was intended and never for an individual employee's personal gain or purpose. If in doubt, employees should seek guidance from their line manager and the Information Governance Team.

Evidential weight relies upon a clear audit trial and the ability to demonstrate that the context and content of information can be relied upon.

The following are key components of use:

- **Retrieval** – information must be accessible throughout its lifecycle for staff with authorised access and in line with access controls;

- **Naming Conventions** – a clear, systematic and consistent standard for naming information is required;
- **Version Control** – a clear, systematic and consistent method of controlling version of information is vital for effective management and efficient working;
- **Storage** - all information must be stored in systematic and consistent to be of use. Storage must also be secure. Further details are provided in the Information Security Policy and the policies and procedures for the relevant systems;
- **Mapped Information Flows** - All flows of personal confidential data (PCD) must be in accordance with legal, regulatory and organisational requirements. Routine flows of information within the organisation and with external bodies will be mapped, ensured as lawful and the risks involved understood.

Maintenance

All information needs to be maintainable through time. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the information is needed, perhaps permanently, despite changes in the format.

Scanning

An important element in meeting the requirement for accessibility and completeness of records is considering which records should be scanned. This is a process that will be addressed on a case by case basis given the expenses involved. However, it is the objective of SEL ICB to ensure all records are in one format (e.g. no hybrid paper – electronic records) with appropriate reference to relevant NHS strategies.

Disposal

Disposal is defined as the management intent for a record once it is no longer required for the conduct of current business. Data and information, not classified as a record, may be destroyed once its business value is concluded.

There are a number of stages in the disposal phase of a corporate record, these include:

- **Closure** - records are made inactive and transferred to secondary storage;
- **Retention** - the retention period varies dependent on the type of information being stored;
- **Destruction** - all information and records must be destroyed appropriately. This applies across all media and to the systems that hold information (such as servers and encrypted memory sticks);
- **Archiving** - upon the end of a retention period, information must be assessed for whether it is requires archiving or destroyed.

Any service that takes over legacy records must manage their disposal. Those that find records within their remit or office space must:

- Register the collection with the Information Governance Team and inform the relevant senior manager for their function to ensure the appropriate Information Asset Owner is identified; and
- Ensure that it is managed appropriately.

Appendix B: Classification Marking of NHS Information

Person-identifiable clinical information should always be held confidentially (*Confidentiality*: NHS Code of Practice). Therefore, the marking OFFICIAL - SENSITIVE: PERSONAL should be used for that kind of information (e.g. patients' clinical records, patient identifiable clinical information, and information about NHS staff that passes between NHS staff, and between NHS staff and staff of other appropriate agencies). This will include patient demographic details that might identify people who have had a GP contact or hospital appointment within a particular timeframe or who may have a particular condition.

NOTE: In order to safeguard confidentiality, the term "OFFICIAL - SENSITIVE: PERSONAL" should never be used on correspondence to a patient.

The endorsement OFFICIAL - SENSITIVE: PERSONAL or OFFICIAL - SENSITIVE: COMMERCIAL should be included at the top centre of every page of the document. Documents so marked should be held securely at all times. That is, they should be stored in a locked room or within secured electronic systems to which only authorised persons have access. They should not be unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed containers and not unattended at any stage. Documents protectively marked that are not in a safe store or transport should be kept out of sight of visitors or others not authorised to view them.

Other uses of endorsement OFFICIAL - SENSITIVE: PERSONAL or OFFICIAL - SENSITIVE: COMMERCIAL:

The endorsement OFFICIAL - SENSITIVE: PERSONAL or OFFICIAL - SENSITIVE: COMMERCIAL should also be used to mark all other sensitive information. That is, material the disclosure of which is likely to:

- Adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals;
- Make it more difficult to maintain the operational effectiveness of the organisation;
- Cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- Prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- Breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- Breach statutory restrictions on disclosure of information; or
- Disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

Information may be classified OFFICIAL - SENSITIVE: PERSONAL or OFFICIAL - SENSITIVE: COMMERCIAL in the light of the circumstances at a particular time. The classification should be kept under review and the information de-classified when the need for this protection no longer applies. NHS use of an equivalent classification for "restricted" is unnecessary when OFFICIAL - SENSITIVE: PERSONAL or OFFICIAL - SENSITIVE: COMMERCIAL is used.

Freedom of Information

When classifying NHS documents, regard should be paid to the requirements of the Freedom of Information Act 2000. Careful consideration should be given before marking documents that would normally be published or disclosed on request. Over-classification might lead to an inappropriate decision not to disclose information that would later be embarrassing to the organisation. For example, where there was an appeal against non-disclosure or the Information Commissioner became involved. Protective markings should wherever possible be restricted to information that would be exempt from disclosure, including temporary exemption, such as that for drafts of documents that are intended for publication.

Further information about the Act and its exemptions (including the application of the "public interest" test) is available in the ICB's Public Access to Information Policy and on the website of the Information Commissioners Office (https://ico.org.uk/).

Principle	Information assets (in any format) will be protectively marked according to the NHS classification. A fundamental of the classification is that protective marking should wherever possible be restricted to information that would be exempt from disclosure under the terms of the Freedom of Information Act 2000. A note of exemptions that are relevant to protective marking is contained in Appendix A.
Creation	Wherever possible, document marking will take place at creation through the use of standard templates. However, where this is not possible, markings can take a number of different forms such as: a stamp, a handwritten annotation or an entry on the container or file cover.
Document Marking	Protective marking classification to be **bold** and in **BLOCK CAPITALS** within the footer of a document or record.
Classification	The NHS does not have a requirement for the full range of protective marking used in the Government Protective Marking Scheme (GPMS). Consequently, SEL ICB will adopt the classifications recommended by the NHS information governance programme. **OFFICIAL** **OFFICIAL-SENSITIVE: COMMERCIAL** **OFFICIAL-SENSITIVE: PERSONAL** The use of UPPERCASE characters is to identify the term is being used in a protective marking context. Any document or record not carrying a protective marking classification will be considered unclassified. Where is it considered appropriate to positively identify and unclassified document the preferred term is NONE. There are two classifications above OFFICIAL in the GPMS: **SECRET** **TOP SECRET**

	NHS staff are not routinely cleared to handle **SECRET** or **TOP SECRET** documents. Any member of staff whom receives material marked with these two classifications should immediately contact the Information Governance Team at IG@selondonics.nhs.uk.
Unclassified **NONE**	Information which is routinely placed in the public domain or general information which requires no access restrictions.
OFFICIAL	This is the default classification for all SEL ICB information. It is expected that normal security measures will be enforced through local processes and therefore provide sufficient levels of protection to information i.e. staff should be sufficiently aware and understand that they have a responsibility for securely handling any information that is entrusted to them.
OFFICIAL-SENSITIVE: PERSONAL	Information marked with this classification will be sensitive information relating to an identifiable individual (or group), where inappropriate access could have damaging consequences.
OFFICIAL-SENSITIVE: COMMERCIAL	Information marked with this classification will be commercial or market sensitive information that could have damaging consequences (for individuals or the ICB) including reputational damage if it were lost, stolen, or inappropriately published.
OFFICIAL-SENSITIVE	In unusual circumstances, OFFICIAL – SENSITIVE information may contain both personal and commercial data, in such cases the descriptor OFFICIAL – SENSITIVE will suffice.
Handling	Detailed handling arrangements for the protective marking classifications in general use within the NHS are contained in the Annexes to this document.
Review	It is recognised that the classification for records is capable of changing over time and will be the subject of periodic review to ensure that the marking applied remains appropriate. It is further recognised that within filing systems a collection of records may be marked **OFFICIAL-SENSITIVE: PERSONAL or COMMERCIAL** (e.g. patient records) but the classification may not apply to the entire contents of the container or file cover.
Sensitive Personal Information	Until such time that SEL ICB captures the protective marking classification of documents or records at creation any document or records that contains personal or sensitive information, the document should be considered OFFICIAL-SENSITIVE: PERSONAL and be handled and stored appropriately. SEL ICB defines sensitive information as: **Information that must be protected because its unauthorised disclosure, alteration, loss or destruction will cause damage to someone or something.** SEL ICB defines personal information as: **Information about an individual whose identity is apparent or can be ascertained from his/her information.** It is recognised that the classification for non-clinical records is capable of changing over time and will be the subject of periodic review to ensure that the marking applied remains appropriate.

Appendix C: Applying a Classification

The following tables have been created to provide SEL ICB staff with a number of questions that they should ask and the appropriate protective marking based upon the response to the question and the assessed risk.

OFFICIAL-SENSITIVE: PERSONAL	S40 Personal Information (may be subject to public interest test)
OFFICIAL-SENSITIVE or OFFICIAL-SENSITIVE: COMMERCIAL	S22 Intended for future publication (including drafts) S30 Investigations and proceedings S31 Law enforcement S38 Endanger health and safety (public interest test) S43 Commercial Interest (public interest test) S44 Legal Prohibitions on disclosure

<u>NOTE: Data protection impact assessments (DPIAs) must be carried out on all personal confidential data held, which includes the requirement to confirm secure storage, use and a risk assessment of the processing.</u>

Protective Marking Handling Matrix

The level of protective marking applied to a document or a record will be the highest level achieved in response to the 7 questions above.

	Classification	
Activity	UNCLASSIFIED/ OFFICIAL	OFFICIAL-SENSITIVE: PERSONAL or COMMERCIAL
Document marking (at creation)	Protective marking classification to be **bold** and in **BLOCK CAPITALS** within the footer of a document or record.	
Hard Copy Storage	General storage no specific barriers required	Stored in lockable room, cabinets or drawers.
Clear Desk Policy	Documents can remain on desk in in-trays etc.	All documents to be locked out of sight when desk is not attended.
Internal Distribution Services	Transit envelopes	Sealed envelope marked prominently with OFFICIAL-SENSITIVE: PERSONAL or COMMERCIAL
External Postal Services and Couriers	Sealed envelope	Confirm recipient name and full address before sending. Include return address, never mark classification on envelope. Consider double envelope for sensitive assets. Consider using registered Royal Mail service or reputable commercial courier's 'track and trace' service .

Office 365 Email @selondonics.nhs.uk	No restriction	Can be sent as encrypted mail to other @selondonics.nhs.uk, NHS Mail and other NHS Digital approved email domains. Guidance for sending secure email (including to patients) - NHS Digital Encryption functions are available through Office365 email. Further guidance is available in the the ICS Email policy and
Email – NHS.net/NHS Digital approved email domains	No restriction	Can be sent as encryption is in place between NHS.net addresses. Further guidance at https://digital.nhs.uk/services/nhsmail/the-secure-email-standard and https://digital.nhs.uk/services/nhsmail/guidance-for-sending-secure-email
Telephone	No restriction	Can be used subject to the usual security checks
Disposal of Protectively Marked Material	Refer to the Department of Health and NHS Retention and Destruction Schedule	

Appendix D: Archiving of documents

It is important that only hard copy records that require storage are sent to archive. Each archive box is charged on a daily basis for storage.

Before hard copy archiving is requested, the following checks should be made:

- Confirmation that the information is not being maintained electronically
- Confirmation that the information needs to be retained in hard copy format (i.e. could it be scanned and saved and any hard copies securely disposed of).
- Check against the SEL ICB Records Retention Schedule or where necessary the NHS Code of Practice, to ensure retention of the documents is absolutely necessary.

  Records Management Code of Practice 2021 - NHS Transformation Directorate (nhsx.nhs.uk)

Co-ordination of records held off site is managed via the SEL ICB corporate governance team, who will act as a central point of contact for contract management with the external records management provider, requests to send records to archive, and requests to retrieve records.

Any requests for guidance should be made by contacting governance@selondonics.nhs.uk.

Process for sending to archive

1. Identify records that require retention but will not need regular, frequent access – this are suitable for sending to off site storage. *NB: it should be noted that there is an additional charge each time a box is requested to be retrieved from IM, so this is not appropriate for records that require frequent access.*
2. Contact governance@selondonics.nhs.uk to advise that there are records to be archived and request an archive box.
3. Place your documentation into the archive box ensuring that items contained in the box are labelled properly. **DO NOT** place box files, hard back folders or plastic wallets into the box. This causes unnecessary waste of stationery, extra weight and makes the destruction of the records more time consuming.
4. Consider the retention of the documents you are storing. Avoid placing items together that need to be kept for 6 years, compared to those that need to be kept for 30 years. You will be storing unnecessary documents for longer periods of time, which will then have storage and cost implications on the organisation.
5. Where the request is for a previously archived box that has been retrieved from our external archive provider to be returned, please go straight to step 8. For new records, continue to step 6.
6. You will need to register the items which are contained in the archive box. To do this please complete the form in appendix A. An electronic copy of the form should be emailed to governance@selondonics.nhs.uk, and a hard copy should be printed out and placed on top of the records in the box. Please ensure all the information is completed as without this detail your archive record will not be traceable.
7. The governance team will advise you of the unique reference number that should be attached to the archive box. Please ensure that this number is written clearly in marker pen on the outside of the box. You should also note the reference number within your own team so if you require this box to be retrieved at a later date you know the reference number to quote.

   You will also need to write the following details on the box:
   - DEPARTMENT NAME
   - DATE OF CONTENTS (TO and FROM)

  - DATE OF DESTRUCTION
  - DATE WHEN THE CONTENTS WERE ARCHIVED
  - NAME OF STAFF ARCHIVING THE DOCUMENTS
  - PLEASE STATE IF THE BOX CONTAINS PERSONAL IDENTIFIABLE INFORMATION (PID) (BY MARKING THE BOX WITH PID)
  - DESIGNATED REFERENCE NUMBER (IM label number)

  All the above information should be written in the spreadsheet as a record that we keep internally. The only three items of information that are written on the archive box are: 1. The department name, 2. The reference number, 3. The IM label which is stuck on the box and on top of the archive box lead.

8. Once this is completed, the governance team should be advised that the box is ready for collection. This may take a few days so space/ arrangements should be made locally for the box to be held securely until collection can be arranged.
9. Prior to collection of the archive boxes, the governance team member responsible will need to check and confirm that the archive box and contents are suitable for archiving. They will provide the label which is stuck on the box and the lead. The references should be checked and confirmed to match what is written in the records book (spreadsheet).

Process for retrieving from archive

1. Check local list to be clear on the reference number of the box you require to be retrieved.
2. Complete the form in Appendix B, with your line managers signature to confirm this box is required – please note there is a cost each time a box is retrieved.
3. Send the completed form to governance@selondonics.nhs.uk
4. The corporate team will make contact with the external archive provider to request retrieval of the box.
5. **Responsibility for ensuring someone is on site to take delivery of the box rests with the local team who requested the information.**
6. Once the box is delivered, confirm receipt by email to governance@selondonics.nhs.uk
7. It is the local teams responsibility to ensure the contents of the retrieved box is stored safely and securely whilst it is on SEL ICB premises.

When requesting a box to be retrieved, enough time should be allowed to enable the requesting process to take place. Therefore, when setting a date for delivery and arranging for a team member to be on site to take delivery of the box, <u>a minimum of two weeks should be given between the date the completed request form is sent to the governance team and the date of delivery requested</u>.

Appendix D1 – archiving request form

NHS SOUTH EAST LONDON INTEGRATED CARE BOARD **ARCHIVING AUTHORISATION FORM**	
Department Name:	
Archiving Officer:	
Date of Archiving:	
Department Box number:	
Content /detail	(Please provide brief content details.
Date of content:	(Date range)
Date of destruction:	(refer to retention schedule)

Please complete the check list below and sign and return this form to the governance team.

		Please tick
1.	The contents of this archive box have been reviewed by a responsible officer and have been placed in the archive box without folders, plastic sleeves or box files.	
2.	The SEL ICB retention schedule or the NHS Code of practice – Records Management Schedule has been referred to when archiving these records to gain the appropriate retention.	
3.	All the appropriate information relating to contents, retention, date, PID, organisation and departmental information has been recorded on the outside of the box and registered on the central archive register.	

4.	Arrangements will be put in place to ensure a local team member is available on site on the designated day of collection to handover the box(es) to the collection driver.	

The above archive box has been checked and its contents and detail are appropriate for archive storage. I hereby authorise the archiving of its contents.

Signed ………………………………………………………………………………………

Managers name: …………………………………………………………………

Date ………………………………………………..

Please send this form to the governance team to arrange for your archive box to be collected.

Appendix D2 – archive retrieval form

NHS SOUTH EAST LONDON INTEGRATED CARE BOARD **ARCHIVED RECORDS RETRIEVAL FORM**	
Department Name:	
Requesting Officer:	
Box reference number:	
Content /detail	(Please provide brief content details.
Requested date of delivery (a local team member to be available to take receipt)	
Likely time period the box will need to be held locally before being returned	
Reason for retrieval /return	

Please complete the check list below to confirm acknowledgement that:

		Please tick
1.	A responsible officer will be on site to take local delivery of the box on the date requested above – if this date is not possible the governance team will arrange for a date as near as possible.	
2.	The receiving team will accept responsibility for the security of the contents of the box whilst it is on SEL ICB premises and in their care.	
3.	Any costs relating to retrieval will be accepted by the department concerned.	

4.	The box will only be held on site for as long as operationally necessary. *Once ready for return, the process for sending to archive above should be followed.*	

Signed ………………………………………………………………………………………

Managers name: …………………………………………………………………

Date ………………………………………………..

Please send this form to the governance team to arrange for your archive box to be requested and delivery arranged.

Appendix E - Equality & Equity Impact Assessment Checklist

This is a checklist to ensure that relevant equality and equity aspects of proposals have been addressed either in the main body of the document or in a separate Equality & Equity Impact Assessment (EEIA)/ Equality Analysis. It is not a substitute for an EEIA which is required unless it can be shown that a proposal has no capacity to influence equality. The checklist is to enable the policy lead and the relevant committee to see whether an EEIA is required and to give assurance that the proposals will be legal, fair and equitable.

The word "proposal" is a generic term for any policy, procedure or strategy that requires assessment.

Equality Analysis Screening Tool

Date of Assessment	14/06/22
Assessor Name(s) & Job Title(s)	Simon Beard, AD Corporate Operations
Organisation	SEL CCG
Name of the project/decision	SEL ICB Information Management Policy
Aim/Purpose of the project/decision	The purpose of this policy is to explain how the ICB will ensure it adheres to national guidance on records retention and appropriate information management.

1. **Do you consider the project/decision to have an *adverse workforce equality impact and/or health inequality impact* on any of the protected groups as defined by the Equality Act 2010? Write either 'yes' or 'no' next to the appropriate group(s).**

Protected group	Yes/No	Protected group	Yes/No	Protected group	Yes/No
Age	No	Pregnancy/Maternity	No	Marriage/Civil Partnership (employment only)	No
Disability	No	Race	No	Socio-economic / Deprivation	No
Gender	No	Religion/Belief	No	Carers	No
Gender reassignment	No	Sexual orientation	No		

2. If you answered ‘yes’ to any of the above give your reasons why

n/a

3. If you answered ‘no’ to any of the above give your reasons why

No anticipated detrimental impact on any equality group. The policy adheres to best practice. This Policy will be applied to all NHS staff employed by the organisation and there is no evidence that the policy will impact, disadvantage or discriminate against any particular protected characteristic group.

4. Please indicate if a Full Equality Analysis is recommended:		**NO**	**YES**
Signature of Project Lead: Simon Beard	Date completed 14/06/22	**NO**	
Signature of reviewing member of Equality Team:	Date reviewed:	**IF YES, BEGIN TO GATHER DATA FOR COMPLETION OF A FULL EQUALITY ANALYSIS**	