RECORDS MANAGEMENT & INFORMATION LIFECYCLE POLICY

# Document Control

| **Document Control Information** | **Details** |
| --- | --- |
| Policy Name | Records Management and Information Lifecycle Policy |
| Policy Number | MSE ICB 012 |
| Version | 1.0 |
| Status | Approved Final Version |
| Author / Lead | Information Governance Lead |
| Responsible Executive Director | Chief Finance Officer and Senior Information Risk Owner |
| Responsible Committee | Audit Committee |
| Date Ratified by Responsible Committee | 20 June 2022 |
| Date Approved by Board/Effective Date | 1 July 2022 |
| Next Review Date | 1 July 2024 |
| Target Audience | All ICB Board members and staff (including temporary/bank/agency/work experience staff, students and volunteers), contractors engaged by the ICS Body, Staff from other MSE ICS Partnership organisations (including those working within ICS Body facilities), Patients and members of the public (visitors, individuals on work experience). |
| Stakeholders engaged in development of Policy (internal and external) | * Information Governance Team. * Information Governance Steering Group. * Audit Committee. |
| Impact Assessments Undertaken | * Equality and Health Inequalities Impact Assessment – completed. |

# Version History

| Version | Date | Author (Name and Title) | Summary of amendments made |
| --- | --- | --- | --- |
| 1 | 01/07/22 | Iain Gear, Information Governance Lead | First version of the policy |
| 1.0 | 07/07/22 | David Triggs, Governance Lead | Final review against policy checklist. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Contents

[1. Introduction 4](#_Toc110000877)

[2. Purpose / Policy Statement 5](#_Toc110000878)

[3. Definitions 6](#_Toc110000879)

[4. Roles and Responsibilities 7](#_Toc110000880)

[4.1. All ICB Employees and Board members 7](#_Toc110000881)

[4.2. Senior Information Risk Owner (SIRO) 7](#_Toc110000882)

[4.3. Caldicott Guardian 7](#_Toc110000883)

[4.4. Information Asset Owner (IAOs) 8](#_Toc110000884)

[4.5. Information Asset Administrators (IAAs) 8](#_Toc110000885)

[4.6. Chief Executive 8](#_Toc110000886)

[4.7. Head of Information Governance 8](#_Toc110000887)

[5. Creation and Management of Records 9](#_Toc110000888)

[5.1. Creation 9](#_Toc110000889)

[5.2. Policy on procedural documents 9](#_Toc110000890)

[5.3. Referencing and naming conventions 10](#_Toc110000891)

[5.4. Filing structures 10](#_Toc110000892)

[5.5. Shared drives 10](#_Toc110000893)

[5.6. Scanning 11](#_Toc110000894)

[5.7. Standards for an Adobe image 12](#_Toc110000895)

[5.8. Tracking and Tracing 12](#_Toc110000896)

[5.9. Secure Transfer of Information and Protective Marking 12](#_Toc110000897)

[5.10. Retention and Disposal 13](#_Toc110000898)

[5.11. Destruction of Records 13](#_Toc110000899)

[5.12. Archiving 14](#_Toc110000900)

[5.13. The Intranet 14](#_Toc110000901)

[5.14. Public Facing Website 15](#_Toc110000902)

[6. Monitoring Compliance 16](#_Toc110000903)

[7. Staff Training 16](#_Toc110000904)

[8. Arrangements for Review 17](#_Toc110000905)

[9. Associated Policies, Guidance and Documents 17](#_Toc110000906)

[10. References 17](#_Toc110000907)

[11. Equality Impact Assessment 17](#_Toc110000908)

[Appendix A - Equality Impact Assessment 18](#_Toc110000909)

[Appendix B – Process Map for Scanning a Document Received Via Post 21](#_Toc110000910)

[Appendix C – Methods of Secure Transfer 22](#_Toc110000911)

[Appendix D – Protective Marking Scheme 26](#_Toc110000912)

[Appendix E – Legal Acts Pertaining to this Document 30](#_Toc110000913)

[Appendix F – Destruction of Records 32](#_Toc110000914)

## Introduction

This policy relates to the MSE Integrated Care Board (the ICB). Records Management and Information Lifecycle relate to the policies, processes, practices, services and tools used by an organisation to manage its information through every phase of its existence, from creation to destruction. Records Management is the process by which the organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal.

The Records Management: NHS Code of Practice has been published by the Information Governance Alliance on behalf of Department of Health as 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. It is based on current legal requirements and professional best practice.

Records within the NHS can be held in paper or electronic form. All NHS organisations will have a duty to ensure that their record systems, policies and procedures comply with the requirements of the Care Record Guarantee.

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. Information has most value when it is accurate, up to date and accessible when needed.

The ICB has written this Policy and is committed to ongoing improvement of records management functions as they believe a number of organisational benefits will be gained from doing so, including:

* + 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 and
  + Archiving and Disposal.

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

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

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

## Purpose / Policy Statement

This policy relates to all records held in any format by the ICB. These include:

* + All administrative records (for example personnel, estates, financial / contracts and accounting and those associated with complaints);
  + All patient health records (for all specialities and including private patients, including x-ray and imaging reports, registers and so on);
  + Computer databases, output and disks and all other electronic records;
  + Material intended for short term or transitory use, including notes and spare copies of documents;
  + Meeting papers, agendas, formal and information meetings including notes taken by individuals in notebooks, bullet points and emails;
  + Audio and video tapes, cassettes and CD Roms
  + Websites and intranet sites that provide key information to patients or service users and staff
  + Text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient or service user) such as Twitter and Skype.

The aim 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;
  + Any action taken to comply with Records Management guidance will not amount to discrimination because of protected characteristics as set out in the Equality Act 2010.

## Definitions

* + Records management – 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;
  + Records lifecycle – describes the life of a record from its creation / receipt through the period of its ‘active’ use, then into a period of ‘inactive’ retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.
  + Records – 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’.
  + Information – a corporate asset. The ICB’s records are important sources of administrative, evidential and historical information. They are vital to the ICB to support their 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 their history and procedures.

## Roles and Responsibilities

### All ICB Employees and Board members

* + 1. Under the Public Records Act every member of staff is responsible for the records they create, receive and use in the course of their duties. Staff should ensure that they comply with this policy at all times and report any breaches through the appropriate incident reporting channels.
    2. Irrespective of its format, all staff must ensure that the following principles are applied to all records created:
  + A consistent definition should be adopted to the creation, use, storage, retrieval, archiving, and disposal of records.
  + All staff should ensure records are stored within a filing structure that reflects the ICB’s business functions. Records must not be retained, disseminated or duplicated unnecessarily.
  + All staff should ensure that records are disposed of by the authorised member of staff and this must be done in accordance with the Records Management Retention and Disposal Schedules.
  + Staff should keep complete and accurate information of all records, activities and transactions and ensure records are captured and managed within the appropriate information and records management systems.
  + Staff should ensure e-mail is only used a source transmission and not for storage.
  + Staff MUST not store information in individual filing systems or on hard drive (that is ’my documents’ or ‘desktop’).

### Senior Information Risk Owner (SIRO)

* + 1. The role of the Senior Information Risk Owner (SIRO) is further described within the ICBs Information Governance Framework and Policy.
    2. The SIRO is responsible for leading on Information Risk and for overseeing the development of an Information Risk Policy.
    3. The SIRO is also responsible for ensuring the corporate risk management process includes all aspects of information risk and for guaranteeing the ICB Board / Governing Body is adequately briefed on information risk issues.

### Caldicott Guardian

* + 1. The role of Caldicott Guardian is further described within the ICBs Information Governance Framework and Policy.
    2. The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients / service-users information and enabling appropriate information sharing.
    3. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to do so, and for advising on options for lawful and ethical processing of information.

### Information Asset Owner (IAOs)

* + 1. Designated Information Asset Owners (IAOs) are senior members of staff at director / assistant director level or heads of department responsible for providing assurance to the SIRO that information risks within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks.
    2. Information Asset Owners are responsible for:
  + Ensuring that all staff within their directorate / department are fully aware of their responsibilities and legal obligations for records management in compliance with policy.
  + Conducting regular audits of records management functions.
  + Reporting policy breaches using the organisation incident reporting mechanism.
  + Ensuring that effective and relevant file management systems are in place for information held within their directorate / department.

### Information Asset Administrators (IAAs)

* + 1. Information Asset Owners can appoint an Information Asset Administrator (IAAs) to support in the management of records with their department / directorate.

### Chief Executive

* + 1. The ICB Chief Executive has overall responsibility for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information.

### Head of Information Governance

* + 1. The Head of Information Governance is responsible for the overall development and maintenance of all records management practices throughout the ICB, in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.
    2. The Head of Information Governance is also the Data Protection Officer for the ICB.
    3. The role of Data Protection Officer is further described within the ICBs Information Governance Framework and Policy.

## Creation and Management of Records

### Creation

* + 1. Records are created to support the day-to-day running of the ICB’s business. A record is created when it meets the legal requirement defined above.
    2. Records created by staff should be arranged in a record keeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information.

### Policy on procedural documents

* + 1. Certain documents such as policies and procedures undergo a consultation process with numerous drafts prior to approval. It is therefore necessary that reference is made to the document version and this is revised with each review using version controls for the management of multiple revisions to the same document to enable the author and other users to identify one version of a document from the other. These include:
  + Keeping successive drafts of the document to provide adequate evidence of the process for example substantial changes during the development of policy.
  + Inserting ‘Draft’ watermarks to indicate the status of the version,
  + Following numbering system by using number with points to reflect minor and major version changes for example. 0.1, 0.2 for minor changes.
  + Changing the final version to v1.0 when the document has reached its ‘Final’ version and continue with 1.1, 1.2 for minor changes to the first version.

| **Version number** | **Summary of changes** | **Author** | **Date** |
| --- | --- | --- | --- |
| 0.1 | Initial draft shown to line manager | Louis Lane | 01/02/2021 |
| 0.2 | Includes comments from line manager – section 2 | Louis Lane | 08/02/2021 |
| 0.3 | Includes comments from the workgroup section 2,5,6 | Louis Lane | 01/03/2021 |
| 0.4 | Correction of grammar and spelling – section 2, 8 | Clark Kent | 10/05/2021 |
| 0.5 | Amendment of section 12 to reflect a procedure change | Louis Lane | 15/09/2021 |
| 1.0 | Change of business unit name and published on the intranet | Kate Moss | 06/01/2022 |

* + 1. The ICB Corporate Lead will be able to advise of the ICB’s Policy Approval process and associated guidelines for formatting of policies.

### Referencing and naming conventions

* + 1. A naming convention is essential for all corporate records. Records should be easily accessible and understandable to staff across the organisation. Corporate records need to follow an agreed naming convention using a systematic approach, for example it should be:
  + easily understood by the staff that create and access records.
  + Alphanumeric.
  + Beginning with key letters or words identifying the directorate.
  + Identifying the department, followed by the business activity.
  + Identifying the document name.
  + Including the initials of the author/creator.
  + Including a version number.
  + Identifying the year of creation.

### Filing structures

* + 1. A clear and logical filing structure that aids the retrieval of records must be used. The filing structure should reflect the way in which paper corporate records are filed to ensure consistency. However, if it is not possible, the names allocated to files and folders should allow ‘intuitive filing’. Filing of the primary corporate record to local drives & desktops on PCs and laptops is not permitted.
    2. The agreed filing structure will also help with the management of the retention and disposal of records.

### Shared drives

* + 1. It is important to consider the content of a document when using this option. Where access to the document is to be limited, the creator of the document must ensure that the record is located in a restricted area on the shared drive.
    2. Similarly, where relevant and appropriate, items should be saved in locations accessible to those in the team that require access and in a logical place with a clear file name. Staff should ensure that any personal folders are not created on their department’s shared drive. Folders created on a shared drive should title the project / content subject name or intents.
    3. Records should not be saved on local / personal drives or personal computers.

### Scanning

* + 1. For the purpose of business efficiency and adapting to paperless innovation, the ICB will consider the option of scanning paper records into electronic format; this will facilitate issues with storage space. Where this is proposed, the following factors will be taken into consideration:
  + The costs of the initial 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 with regard to records which may have archival value, as the value may include the format in which it was created;
  + 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’.
    1. Images must adhere to the following standards;
  + Every image must be a true representation of the original document
  + All text must be legible.
  + The patient / staff member associated with the document must be clear on the scanned image.
  + All images received from an external source must be date stamped when received, before scanning into electronic form. This must be clear on the scanned document.
  + There must be an audit trail on the system of the date and time when the image was scanned into the system.
  + There must be a completed audit trail of information detailing who scanned and saved the image into the system, inclusive of time and date.
  + The image should be saved to a suitable agreed resolution to ensure quality.
  + An audit trail must be kept detailing destruction of any documents. The best practice process would be to retain the original information with the scanned image.
    1. For a process map to scan a document received via post, please see Appendix B.

### Standards for an Adobe image

* + 1. Documents may be converted into an ‘Adobe’ image and saved like a scanned image. However, images must adhere to the following standards:
  + Every image must be a true representation of the original document.
  + All text must be legible.
  + The patient / staff member associated with the document must be clear on the image.
  + There must be an audit trail on the system of the date and time when the image was saved into the system.
  + There must be an audit trail of who saved the image into the system.
  + The image should be checked before it is saved to ensure quality.

### Tracking and Tracing

* + 1. Tracking and tracing procedures implemented must enable the movement and location of records to be controlled. This will provide an auditable trail of record transactions.
    2. The process need not be a complicated one, for example, a tracking procedure could comprise of a book that staff members sign when a corporate record is physically removed from, or returned to, its usual place of storage (not when a record is simply removed from a filing cabinet by a member of staff from that department as part of their everyday duties).
    3. Tracking mechanisms to be used should include:
  + the item reference number or identifier;
  + a description of the item (for example the file title);
  + the person, position or operational area / team who may have possession of the item;
  + the date and time of movement that took place.

### Secure Transfer of Information and Protective Marking

* + 1. It is important that when information needs to be shared, it is transferred and / or transported in a secure and efficient manner. There are many different methods of transferring information and it is vital that the most appropriate method is chosen, dependent on the type of information to be transferred.
    2. For more information on methods of secure transfer, please see Appendix C.
    3. Government Security Classifications have been implemented to assist in deciding how to share and protect information. Three simplified levels of security classifications for information assets are now in effect.
    4. Details of classifications can be found on Appendix D.

### Retention and Disposal

* + 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 the ICB’s business functions.
    2. The ICB has adopted the retention periods set out in the Records Management: NHS Code of Practice for Health and Social Care 2021.

### Destruction of Records

* + 1. Where a document / record has reached its retention date it should be considered for destruction. The process is as follows:
  + Review by an appropriate clinician; head of service or a senior manager, to ensure that the records are not needed beyond their listed retention period. If records could be of particular public interest, they should also be considered for archival preservation with The National Archives. The reviewer should sign the ‘Destruction of Records’ sheet (Appendix F) to demonstrate they are happy with the records being destroyed.
  + If documents are stored in an off-site archive, checking the index list of the documents should generally be sufficient (with input from appropriate staff members where needed). If it is not clear what is in a document, this should be recalled from the archive so a more thorough check can take place.
  + The ‘Destruction of Records’ sheet (Appendix F) should also be confirmed and signed off by the Caldicott (for patient records) or the SIRO (for corporate records) so destruction can be progressed.
  + Secure destruction should be arranged.
  + If the documents to be destroyed are with an off-site archive provider, they usually have process in place to destroy boxes on your behalf. They will provide a certificate of destruction for those documents / boxes that have been destroyed.
  + If the documents to be destroyed are on-site (either archived on site, recalled from off-site archive, or had been stored within the ICBs offices) destruction should be done separately to your usual confidential waste disposal, but can be done by the same company and at the same time. The disposal company will need to provide a certificate of destruction relating to just those documents that have been disposed of, i.e. separate to any certificate that comes with your usual confidential waste disposal.
  + A log of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the Records Manager, so that the organisation is aware of those records that have been destroyed and are therefore no longer available.
    1. If a record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place or, if the authority has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act have been exhausted or the legal process completed.

### Archiving

* + 1. Once a record has ceased to be accessed regularly, for example if the member of staff has left the organisation or the record refers to a historic business activity, it is necessary for the practical operation of the organisation that this then should be archived to an alternative storage location.
    2. The ICB has adopted the retention periods detailed within the Records Management Code of Practice for Health and Social Care 2021 Section 4 Retention Schedule: Retention Schedule. The retention schedule details the minimum retention period for each type of record. Records, whatever the media, may be retained for longer than the minimum period, however this requires formal approval of the Information Governance Steering Group (IGSG). They should not however be retained for more than 30 years. Where a period longer than 30 years is required (for example to be preserved for historical purposes), or for any pre-1948 records, the National Archives should be consulted.
    3. It should be noted that records containing personal information are subject to the Data Protection Act 2018. Section 90 sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary).
    4. If a particular record is not listed in the schedules the Information Governance Lead should be contacted for advice.

### The Intranet

* + 1. The Intranet is a web-based communication tool. It has been set up in a centralised location to enable staff to easily locate any materials that they may need. This is to help them carry out their duties or to generally find out more information on a particular subject.
    2. Examples of information which should be published on the Intranet are:
  + Policies, Procedures and Strategies.
  + Forms.
  + Contact Lists.
  + Minutes of Meetings.
  + General Information.
  + Newsletters.
    1. Examples of information which should not be published on the Intranet are:
  + Confidential Information.
  + Patient / Personal Information.
  + Commercially Sensitive Information.
  + Incomplete Information for example. draft documents.

### Public Facing Website

* + 1. Information that is intended to be made publicly available should be published through the Freedom of Information (FOI) Publication scheme located on the Public Facing Website. Requests for new content to be added should be made via the IG Lead / FOI Co-ordinator.
    2. Examples of information which should be routinely published on the public facing website are:
  + The ICB Annual Report.
  + Press Releases.
  + Up to date contact Information for the ICB.
  + Information about services provided by the ICB.
  + A list of the main categories of Information that have been most frequently requested via the FOIA.
  + A list of data sets requested previously under the FOIA.
    1. Examples of information which should not be published on the public facing website are:
  + Person Identifiable Information of any description.
  + Confidential Reports.
  + Commercially Sensitive Information.
  + Incomplete Information for example draft documents, any information not approved or finalised.

## Monitoring Compliance

The ICB will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following two methods:

IG Incidents – Information Governance compliance will be monitored quarterly through the review of reported IG incidents by the IG Steering Group.

The IG Steering Group has a responsibility to provide assurances that this framework is adequate for providing clear guidance in the event of significant changes which may affect it. The Head of Information Governance will ensure that adequate arrangements exist for:

* + Reporting incidents, Caldicott issues.
  + Analysing and upward reporting of incidents and adverse events.
  + Reporting IG work programs and progress reports.
  + Reporting Data Security and Protection Toolkit (DSPT) assessments and improvement plans.
  + Communicating IG developments.

Information Asset Registers – The ICB undertakes regular monitoring and gap analysis through the Information Asset Register work-stream.

This policy will be published on the ICB website. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels for example through e-mail, in bulletins and so on.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

## Staff Training

All staff (permanent, temporary, contract or seconded) likely to be in post for 3 months or longer, are required to complete the online mandatory IG training module- Data Security Awareness Level 1 within the first month of employment (or within two weeks of joining if they work with person identifiable information).

The Data Security Awareness Level 1 e-learning module can be accessed either through ESR (https://my.esr.nhs.uk/) or e-learning for health (https://www.e-lfh.org.uk/).

Further training is required for staff who process personal information, and staff within specific roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of effective delivery of training program.

## Arrangements for Review

This policy will be reviewed no less frequently than every two years. An earlier review will be carried out in the event of any relevant changes in legislation, national or local policy/guidance, organisational change or other circumstances which mean the policy needs to be reviewed.

If only minor changes are required, the sponsoring Committee has authority to make these changes without referral to the Integrated Care Board. If more significant or substantial changes are required, the policy will need to be ratified by the relevant committee before final approval by the Integrated Care Board.

## Associated Policies, Guidance and Documents

The following documentation relates to the management of information and together underpins the ICB’s Information Governance Assurance Framework. This policy should be read in conjunction with other IG policies & the IG Resource Guide:

* + Information Governance Framework and Policy.
  + Access to Information Policy.
  + Information & Cyber Security Policy.
  + Information Sharing Policy.
  + IG Resource Guide.

## References

Please see Appendix E for information of related Legal Acts

## Equality Impact Assessment

The EIA has identified no equality issues with this policy.

The EIA has been included as Appendix A.

## Appendix A - Equality Impact Assessment

#### Assessor’s Name: Iain Gear

#### Assessor’s Job Title: Information Governance Lead

#### Date: 10th May 2022

#### Outcomes

Briefly describe the aim of the policy and state the intended outcomes for staff.

The Records Management Policy will support the organisation and its staff to achieve legislative requirements in relation to the effective management of records.

#### Evidence

What data/information have you used to assess how this policy might impact on protected groups?

The ICB regularly monitor the make-up of the workforce, including protected groups.

Who have you consulted with to assess possible impact on protected groups? If you have not consulted other people, please explain why?

Mid and South Essex Information Governance Steering Group; Mid and South Essex Audit Committees meeting in common; Human Resources.

#### Analysis of impact on equality

The Public Sector Equality Duty requires us to **eliminate** discrimination, **advance** equality of opportunity and **foster** good relations with protected groups. Consider how this policy / service will achieve these aims.

N.B. In some cases it is legal to treat people differently (objective justification).

* **Positive outcome** – the policy/service eliminates discrimination, advances equality of opportunity and fosters good relations with protected groups.
* **Negative outcome** – protected group(s) could be disadvantaged or discriminated against.
* **Neutral outcome** – there is no effect currently on protected groups.

Please tick to show if outcome is likely to be positive, negative or neutral. Please fill all boxes, any that aren’t applicable enter N/A.

Consider direct and indirect discrimination, harassment and victimisation.

| Protected  Group | Positive  outcome | Negative  outcome | Neutral  outcome | Reason(s) for outcome |
| --- | --- | --- | --- | --- |
| Age |  |  | X | The policy refers to ensuring that “any action taken to comply with Records Management guidance will not amount to discrimination because of protected characteristics as set out in the Equality Act 2010.” |
| Disability  (Physical and Mental/Learning) |  |  | X | As above |
| Religion or belief |  |  | X | As above |
| Sex (Gender) |  |  | X | As above |
| Sexual  Orientation |  |  | X | As above |
| Transgender/Gender Reassignment |  |  | X | As above |
| Race and ethnicity |  |  | X | As above |
| Pregnancy and maternity (including breastfeeding mothers) |  |  | X | As above |
| Marriage or Civil Partnership |  |  | X | As above |

#### Monitoring Outcomes

Monitoring is an ongoing process to check outcomes. It is different from a formal review which takes place at pre-agreed intervals.

What methods will you use to monitor outcomes on protected groups?

The ICB undertakes regular monitoring and gap analysis through the Information Asset Registers, Data Protection Impact Assessments and IG related incident investigations.

#### Review

How often will you review this policy / service?

Every two years.

## Appendix B – Process Map for Scanning a Document Received Via Post



## Appendix C – Methods of Secure Transfer

Mark the envelope “Private & Confidential - To be opened by Addressee Only.”

Confirm the name, department, and address of the recipient

Seal the information in a robust envelope.

When appropriate, send the information by registered post or courier

Ask the recipient to confirm receipt.



**information by POST**



**information by TELEPHONE**

Take a contact telephone number

e.g. main switchboard number

(never a direct line or mobile telephone number).

Confirm the name, job title, department

and organisation of the person requesting the information.

Confirm the reason for the information request if appropriate.

Check whether the information can be provided. If in doubt, tell the enquirer you will call them back.

Provide the information only to the person who has requested it

(do not leave messages).

Ensure that you record

your name, date and the time of disclosure, the reason for it and who authorised it.

Also record the recipient’s name, job title, organisation and telephone number.



**information by FAX**

Telephone the recipient of the fax

(or their representative)

to let them know you are going to send confidential information.

Ask them to acknowledge receipt of the fax

Use

pre-programmed numbers wherever possible.

**This guidance relates to**

**Data Protection Principle 7**

**and**

**Caldicott Principle 4**

Double check the fax number

Make sure your fax cover sheet states who the information is for and mark it “Private and Confidential.”

If appropriate, request a report sheet to confirm that transmission was OK.

**If you are faxing to a known Safe Haven or Secure Fax, you do not need to follow any special instructions.**

**If not follow steps 1-6**



**Guidance for TRANSPORTING**

**personal information**

Personal identifiable information should only be taken off site when absolutely necessary, or in accordance with local policy.

Record what information you are taking off site and why, and if applicable, where and to whom you are taking it.

Information must be transported in a sealed container, bag etc.

Never leave personal identifiable information unattended.

Ensure the information is returned back on site as

soon as possible.

Record that the information

has been returned.

## Appendix D – Protective Marking Scheme

Classification of NHS Information - Marking Guidance for ICBs.

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

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

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

OFFICIAL

Definition – ALL routine public sector business, operations and services should be treated as OFFICIAL. The ICB will operate exclusively at this level including the subset categories of OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL–SENSITIVE: PERSONAL where applicable. See Table 1 for examples.

SECRET

Definition – Very sensitive government (or partners) information that requires protection against the highly capable threats, such as well- resourced and determined threat actors and highly serious organised crime groups.

TOP SECRET

Definition – Exceptionally sensitive Government (or partners) information assets that directly support (or threaten) the national security of the UK or allies and requires extremely high assurance or protection against highly bespoke and targeted attacks.

There is no need to apply the new classification procedure retrospectively.

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

All information used by the ICB is by definition ‘OFFICIAL.’ It is highly unlikely the ICB will work with ‘SECRET’ or ‘TOP SECRET’ information.

Things to remember about OFFICIAL information:

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

A limited subset of OFFICIAL information could have more damaging consequences if it were accessed by individuals by accident or on purpose, lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL

classification tier, but should have additional measures applied in the form of OFFICIAL- SENSITIVE.

This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic documents/records.

In additional to the marking of OFFICIAL-SENSITIVE further detail is required regarding the

content of the document or record, i.e.OFFICIAL – SENSITIVE: COMMERCIAL

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

Or

OFFICIAL – SENSITIVE: PERSONAL

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

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

In unusual circumstances OFFICIAL – SENSITIVE information may contain both Personal

and Commercial data, in such cases the descriptor OFFICIAL – SENSITIVE will suffice.

NHS Confidential

The ICB has adopted the government classification scheme for corporate information as it is an expectation from the DH for all Arms Length bodies (ALBs) to comply with. Our approach will satisfy any corporate communications with DH, other departments and ALBs. In the interim, some NHS organisations may still work to existing IG guidance; consequently any information received from an NHS organisation may be marked as NHS Confidential which should then be treated as OFFICIAL – SENSITIVE depending on its type.

How to handle and store OFFICIAL information;

EVERYONE is responsible to handle OFFICIAL information with care by:

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

How to handle and store OFFICIAL – SENSITIVE information;

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

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

* + Always apply appropriate protection and comply with the handling rules.
  + Always question whether your information may need stronger protection.
  + Make sure documents are not overlooked when working remotely or in public areas, work digitally to minimise the risk of leaving papers on trains, etc.
  + Only print sensitive information when absolutely necessary.
  + Send sensitive information by the secure email route or use encrypted data transfers.
  + Encrypt all sensitive information stored on removable media particularly where it is outside the organisation’s physical control.
  + Store information securely when not in use and use a locked cabinet/drawer if paper is used.
  + If faxing the information, make sure the recipient is expecting your fax and double check their fax number.
  + Take extra care to be discreet when discussing sensitive issues by telephone, especially when in public areas and minimise sensitive details.
  + Do not send to internet email addresses e.g. Gmail, Hotmail, etc.
  + Only in exceptional cases, where a business need if identified, should sensitive information be emailed over the internet, in an encrypted format, to the third parties. Contact the Corporate IG team for further advice.
  + The use of pin code for secure printing is both widely available and preferable way to manage the printing process.

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

| **Category** | **Definition** | **Marking** |
| --- | --- | --- |
| Appointments | Concerning actual or potential appointments not yet announced | OFFICIAL- SENSITIVE: COMMERCIAL |
| Barred | Where there is a statutory (Act of Parliament or European Law) prohibition on disclosure.  disclosure would constitute a contempt. of Court (information the subject of a court order). | OFFICIAL- SENSITIVE: COMMERCIAL |
| Board | Documents for consideration by an organisation’s Board of Directors, initially, in private.  (Note: This category is not appropriate to a document that could be categorised in some other way). | OFFICIAL- SENSITIVE: COMMERCIAL |
| Commercial | Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs. | OFFICIAL- SENSITIVE: COMMERCIAL |
| Contracts | Concerning tenders under consideration and the terms of tenders accepted. | OFFICIAL- SENSITIVE: COMMERCIAL |
| For Publication | Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date. | OFFICIAL- SENSITIVE: COMMERCIAL |
| Management | Concerning policy and planning affecting the interests of groups of staff.  (Note: Likely to be exempt only in respect of some health and safety issues). | OFFICIAL- SENSITIVE: COMMERCIAL |
| Patient Information | Concerning identifiable information about patients. | OFFICIAL- SENSITIVE: PERSONAL |
| Personal | Concerning matters personal to the sender and/or recipient. | OFFICIAL- SENSITIVE: PERSONAL |
| Policy | Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published). | OFFICIAL- SENSITIVE: COMMERCIAL |
| Proceedings | The information is (or may become) the subject of, or concerned in a legal action or investigation. | OFFICIAL- SENSITIVE: COMMERCIAL |
| Staff | Concerning identifiable information about staff. | OFFICIAL- SENSITIVE: PERSONAL |

## Appendix E – Legal Acts Pertaining to this Document

**The Data Protection Act 2018:** all staff must abide by the Data Protection Act 2018 which controls how personal information is used. It incorporates the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED).

Personal information relating to staff, suppliers, etc. may only be accessed and used by staff on a need to know basis. Unauthorised disclosure of such “personal data” may result in disciplinary action and prosecution. Under the Act, Article 5 states personal data must be:

* Processed fairly, lawfully and in a transparent manner;
* Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
* Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
* Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
* Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
* Processed in a manner than ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Every individual, including staff are entitled to be informed of any personal data held on them by the organisation, to access that data and to have it corrected if it is inaccurate All enquiries relating to the Data Protection Act must be referred to the Data Protection Officer.

* **The Public Records Act 1956 and 1967 and Freedom of Information Act 2000:** These Acts regulate the storage and publication of records held by public bodies.
* **The Copyright, Designs and Patents Act 1988**: It is illegal to copy, without the appropriate consent, software except for backup purposes, and each machine must have a license for its software. The copyright owner has the right to bring civil proceedings and in certain circumstances criminal proceedings against those that infringe their rights.
* **Department of Health Guidance:** Guidance and standards for the Protection and Use of Patient Information and Caldicott Guardian guidance can be found on the Department of Health website.

## Appendix F – Destruction of Records

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ICB Department: | | | | | | |
|  | | | | | | |
| Description of records: |  | | | | | |
|  | | | | | | |
| Reviewing clinician / Head of service / Senior manager name. | | | | | | |
|  | | | | | | |
| Reviewing the information: | *Please put* ***X***  *in the appropriate box below* | | | | | |
| I confirm that these documents / boxes have been reviewed and are no longer required | | | | |  | |
|  |  | | | | | |
| I confirm that these records have been reviewed and should be kept. | | | | |  | |
| The records should be reviewed again after a period of | |  | months / years | | | |
| Signature | Date | | | | | |
|  |  | | | | | |
| Confirmation of destruction by | *Please put* ***X***  *in the appropriate box below* | | | | | |
|  | Caldicott | |  |  | | |
|  | SIRO | |  |  | | |
| Name |  | | | | | |
|  | | | | | | |
| By signing this you are confirming that you agree with the opinion above and that these records should: | | | | | | |
|  | *Please put* ***X***  *in the appropriate box below* | | | | | |
| Be kept and reviewed again after the period mentioned above. | | | | | |  |
| Be offered to The National Archives for archival preservation. | | | | | |  |
| Be securely destroyed. | | | | | |  |
|  |  | | | | | |
| Signature | Date | | | | | |
|  |  | | | | | |