HSE National Information Classification and Handling Policy

2027 - 2030

National Policy ☒ National Procedure ☐ National Protocol ☐ National Guideline ☐
National Clinical Guideline ☐

HSE National Information Classification and Handling Policy

DOCUMENT GOVERNANCE	
Document Owner (post title):	National Director, Public Involvement, Culture and Risk Management
Document Owner name:	Joe Ryan
Document Owner email: (Generic email addresses only accepted)	nrrp@hse.ie
Document Commissioner(s): (Name and title of post holder):	Joe Ryan, National Director
Date Document Approved: (Formal ratification by the Governance/Steering Group)	20/10/2026
Document Approved by: (Name and title of post holder)	HSE Senior Management Team
Document Approver Sign-Off: (e-signature)	
Development Group Name:	HSE National Records Management Programme working Group
Development Group Chairperson:	Ann Sheehan

DOCUMENT MANAGEMENT			
Date effective from:		05/04/2027	
Date set for next review:		05/04/2030	
Your Reference No: *(if applicable)*		n/a	
Current version no:	Version 2.0	**Archived version no:**	1.0

VERSION CONTROL UPDATE		
Version No.	**Date reviewed**	**Comments**
2	01/10/2026	A full Policy update in line with National Template for Developing HSE National Policies, Procedures, Protocols, Guidelines (PPPGs) and HSE National Clinical Guidelines.
1	01/02/2013	1.0 HSE Information Security Project Board (ISPB)

PUBLICATION INFORMATION
Topic:
Information Management
National Group:
HSE National Records Management Steering Group
Short summary:
This national policy (“the policy”) provides guidance on the HSE National Information Classification and Handling Policy which fits within HSE information security programme and complements HSE’s data management and records management programmes.
Description:
This policy has been developed to assist the HSE in applying a degree of sensitivity and criticality to all the information created, collected, processed and disseminated within the organisation. The classification assigned places controls relating to the type of information and its need to remain confidential and secure.

Table of Contents

1. Background and purpose 5

2. Scope 7

3. Definitions 9

4. Policy 12

4.1 Information Classification 12
4.1.1 Public Information 12
4.1.2 Internal Information 13
4.1.3 Confidential Information 14
4.1.4 Restricted Information 15
4.1.5 Note re Medical Record Types 16
4.2 Information Classification Matrix 17
4.3 Information Handling 19

5. Roles and Responsibilities 20

5.1 Information Owners 20
5.2 Line Managers 20
5.3 Staff 21
5.4 Contractors, Sub-contractors and Agency Staff 21
5.5 Third party commercial service providers 21

6. Policy Governance and Implementation 22

6.1 Disclosure of interests 22
6.2 Methodology 22
6.3 Consultation and Review Process 22
6.4 National implementation plan 23
6.5 Governance and approval 24
6.6 Monitoring and audit 24
6.7 Policy review and update 24

7. References 25

8. Appendices 27

8.1. Appendix I: Information Handling Matrix 27
8.1.1 Information Classification & Handling Procedures: General Handling 27
8.1.2 Records Retention – Defined Storage Locations 31
8.1.3 Storage of and Access to of Electronic-Based Information 37
8.1.4 Storage of Paper & Film Based Information 44
8.1.5 Transfer, disclosure and sharing of information: spoken word and post 46
8.1.6 Transfer, disclosure and sharing of information: electronic means 48
8.1.7 Physical Security 57
8.1.8 Destruction & Disposal of Information 59
8.2 Appendix II: National Implementation Plan 62
8.3 Appendix III: Audit Checklist for the Implementation of the HSE National Records Retention Policy 63
8.4 Appendix IV: National Records Management Programme Group Membership 65
8.5 Appendix V: Membership of Approval Governance Group 66
8.6 Appendix VI: Signature sheet 67

1. Background and purpose

HSE creates, collects, processes, stores, shares and disposes of significant volumes of information in multiple formats in the delivery of health and social care services. Protecting the confidentiality, integrity, and availability of these information assets throughout their lifecycle is fundamental to maintaining public trust, safeguarding service users, supporting clinical care, and ensuring effective service delivery.

The HSE is committed to the correct and proper classification, handling, storing and destroying information. Information classification helps determine the sensitivity level of an information asset and thereby, the information security controls which must be applied to handle the information asset appropriately and protect the asset through its lifecycle.

This Information Classification and Handling Policy establishes a consistent framework for classifying and managing HSE information according to its sensitivity, business value, legal obligations and records management requirements. Information classification does not determine how long information is retained. Retention periods are determined solely by the HSE National Records Retention Policy (NRRP) and approved retention schedules.

The policy supports the HSE's commitment to information governance, cyber security, data protection and records management by ensuring that information receives appropriate levels of protection, information security controls when handling the asset during its lifecycle including creating or collection the information, storing it, accessing and using the information, retaining the information after use, and finally, securely disposing of it.

All staff should be aware of and consider related HSE policies on the appropriate handling of information, ICT and information storage assets, including but not limited to:

HSE Information Technology (IT) Security Policy
HSE Electronic Communications Policy
HSE Information Technology (IT) Acceptable use Policy
HSE Password & Passcode Policy
HSE Encryption Policy
HSE National Records Retention Policy 2025-2028 (NRRP)
HSE Standards and Recommended Practices for Healthcare Records Management v3.0 2011

HSE Data Protection Policy 2025

HSE National Manual Handling and People Handling Policy 2025

HSE Child Protection and Welfare Policy Guide 3: Managing Child Protection and Welfare Records

When classifying and handling information assets, HSE staff should consider legislation on Data Protection, Freedom of Information, and any other legislation, regulations, or professional codes of conduct on the appropriate governance of information, including legislation for specific domains of information (e.g. health and social care, financial, HR, public sector, etc.). See HSE National Records Retention Policy for guidance on legislative and regulatory requirements.

The appropriate classification, handling and storage of information is the responsibility of each HSE staff member. This policy is mandatory and applies to all HSE staff, students, contractors, sub-contractors, agency personnel and third parties that have access to HSE information.

2. Scope

This policy represents the HSE's national position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to the following.

HSE information in physical or electronic formats including:

- All electronic records held by HSE in cloud storage, in on-premise networked servers, and offline on ICT devices;
- All physical (paper-based) records including patient charts, handwritten notes, printed reports and archived files; and
- All hybrid records (paper converted to digital and vice versa).

All individuals handling HSE information assets including:

- HSE departments, directorates and service areas;
- HSE staff and students;
- HSE contractors and sub-contractors;
- Agency personnel working on behalf of the HSE; and
- Third party commercial service providers.

Note that where this policy refers to 'HSE staff' or 'HSE staff member', the direction also applies to all individuals listed above.

All locations and devices where HSE information assets are held:

- On-site storage facilities;
- Off-site storage facilities;

- Offline ICT devices;
- Online ICT servers and devices on the HSE network;
- HSE tenants in third party cloud services (e.g. HSE's tenant of Microsoft 365); and
- Any approved multi-tenant locations in third party cloud services which HSE licenses.

The full lifecycle of an information asset from when it is first created or collected through to storage, indexing, access, search and retrieval, use, subsequent retention after use, and final destruction or transfer to long-term archive.

The following are out of scope.

This policy does not cover recommended practices for healthcare record management. See HSE Standards and Recommended Practices for Healthcare Records Management v3.0 2011.

This policy does not cover guidelines on backup of essential information and the recovery of systems in the event of data loss, system failure, or other unforeseen incidents. See National HSE Policy for Backup and Restore, which includes a schedule for regular backups and a retention policy specifying the duration and criteria for retaining backup data, aligning with regulatory requirements and best practices.

HSE staff should consult HSE National Records Retention Policy and National Records Management Programme guidance and templates for the appropriate management of HSE records relative to retention, disposition review, and lifecycle management. Of note, the programme provides guidance on the identification and handling of historical records of archival value. The National Records Management Programme is chaired by the National Director for Public Involvement, Culture and Risk Management.

3. Definitions

Anonymised data	The data has been stripped of all personally identifiable information, therefore making it impossible to trace back to an individual. Fully anonymised data is not considered personal data and is therefore outside the scope of the GDPR.
Archival value	Records possessing enduring historical, evidential, legal, cultural, research or organisational value that warrant permanent preservation beyond their operational use and retention period.
Authorisation / Authorised	Official HSE approval and permission to perform a particular task.
Backup	The process of taking copies of information and data to use in the event that the original information and data are lost, stolen or destroyed.
Breach of Confidentiality	The situation where HSE confidential or restricted information has been put at risk of unauthorized disclosure as a result of the loss or theft of the information or, the loss or theft of a computer device containing a copy of the information, or through the accidental or deliberate release of the information.
Disposition Review	A documented assessment undertaken when a record reaches the end of its retention period to determine whether it should be destroyed, retained for a further period, or transferred for archival preservation.
Electronic Media	Any information that has been created and is stored in an electronic format, including but not limited to software, electronic documents, photographs, and video and audio recordings.
Encryption / Encrypt	The process of converting (encoding) information from a readable form (plain text) that can be read by everyone into an unreadable form (cipher text) that can only be read by the information owner and other authorised persons.
Encryption Key	A piece of information (parameter usually a password) used to encrypt/decrypt information.
HSE Network	The data communication system that interconnects different HSE network resources, Local Area Networks (LAN), Wide Area Networks (WAN), Wi-Fi Wireless Networks and the National Health Network (NHN). Includes all HSE network domains, sub

	networks (sub-nets), and perimeter networks which are managed directly by the HSE, and those managed by commercial third-party service providers or others on behalf of the HSE.
HSE Network Server	A computer on the HSE network used to provide network services and/or manage network resources.
Incinerate	Destruction by burning.
Information	Any information irrespective of the format that is capable of being processed or has already been processed.
Information Owner	The individual responsible for the management of a HSE region, directorate or service (i.e. HSE Regional Director of Operations (RDO), or National Director or equivalent).
Information System	A computerised system, application, database or service used to process (i.e. collect, store, share, disseminate) information and data, for the purposes of supporting decision making.
Master record	The master record is the single authoritative version of a record, designated by the business owner as the official record. The master record must be retained within an approved system of record and managed in accordance with the HSE National Records Retention Policy. Retention obligations apply to the master record; duplicate and reference copies should be disposed of when no longer required for operational use.
Microsoft 365 / M365	Microsoft 365 or M365 is a cloud-based platform to support HSE productivity, communication and collaboration. This policy details how information should be stored, accessed and shared from HSE's M365 tenant (i.e. HSE's own licensed instance of the M365 platform). The policy includes how information should be handled in M365 Teams, SharePoint, OneDrive and Exchange Email.
Record	A record is information created, received, and maintained as evidence of business activities, decisions, or transactions, and as an organisational asset. To be considered an authoritative record, it must be authentic, reliable, have integrity, and be usable. • **Authenticity** means the record can be proven to be what it purports to be.

	• **Reliability** means the record can be trusted as a full and accurate representation of the activity or transaction it documents. • **Integrity** means the record is complete and unaltered, with any authorised amendments clearly identified. • **Usability** means the record can be located, retrieved, presented, and interpreted for as long as it is required.
Removable Storage Media	Any portable storage device or media, including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick/pen/keys), and external/portable hard drives.
Third Party	Any individual who is not a HSE employee, student, employed jointly by the HSE and another organisation (i.e. joint appointments) or on secondment to the HSE from another organisation. For the avoidance of doubt, third parties shall include, but are not limited to, commercial third-party service providers and their employees, HSE funded agencies and their employees (with the exception of those who are on secondment to the HSE or are 'joint appointments').
Users	Any authorised individual who uses the HSE Information Technology (I.T.) resources.
VPN (Virtual Private Network)	A mechanism used to create a secure connection between a remote computing device and a computer network, or between two computer networks, connecting through a public network (e.g. the internet). The VPN creates an encrypted tunnel between the remote computing device (or network) and the computer network.
Web content	Shall mean information in all formats (e.g. text, images, audio or video) published on the internet.

4. Policy

4.1 Information Classification

All information (irrespective of its format) owned, created, received, stored and processed by the HSE must be classified by the sensitivity of its contents. Classification controls should consider the organisational needs for sharing or restricting the information and the associated impacts and risks (e.g. consequences if information is handled inappropriately). All information owned, created, received, stored or processed by the HSE must be classified into one of following categories:

Public
Internal
Confidential
Restricted.

4.1.1 Public Information

Public information is defined as information that is available to the general public and is intended to be distributed outside the HSE. There would be no impact on the HSE, its staff, clients or patients if this type of information was mishandled or accidentally released. Some examples of public information include:

Patient / client brochures,
Staff brochures,
News / media releases,
Pamphlets,
Advertisements,
Web content,
Job postings, and
Public health information.

4.1.2 Internal Information

Internal information is defined as information that is only intended to be distributed internally among HSE staff, students, contractors, sub-contractors, agency staff and authorised third parties (i.e. service providers, etc). It should only be shared with authorised people inside the HSE or approved partners who need it for their work on behalf of HSE. In the majority of instances there would be no significant impact on the HSE, its staff, clients or patients if this type of information was mishandled or accidentally released however it should still be protected and not shared publicly. Some examples of internal information include:

Internal contact directory;
Intranet content and SharePoint Communication Sites;
Internal policies and procedures (excluding those published on the HSE website);
User manuals;
Training manuals and documentation;
Staff newsletters and magazines;
Inter-office memoranda (depending on the content);
Business continuity plans;
Internal audit preparation material;
Draft operational planning documents; and
Non-sensitive internal emails.

4.1.3 Confidential vs Restricted Information

4.1.3.1 Confidential Information++

Confidential information is information protected by legislation, regulation, professional obligations, contractual requirements, or HSE policy, where unauthorised disclosure could reasonably cause harm, distress, financial loss, reputational damage, operational disruption, or a breach of legal obligations.

Confidential information should be accessible only to authorised individuals with a legitimate business, clinical, operational or legal need to know.

4.1.3.2 Restricted Information

Restricted information is a subset of Confidential information requiring enhanced protection because unauthorised disclosure would be expected to result in significant harm to an individual, substantial legal or regulatory consequences for the HSE, serious reputational damage, or increased risk to vulnerable persons.

The classification should be based on the potential impact of disclosure rather than the type of system or storage location used.

Restricted information should only be accessible to individuals with a demonstrable and specific need to know and should be subject to enhanced access controls, monitoring and handling requirements.

Classification is determined by the sensitivity and impact of unauthorised disclosure, not by the information system, application, storage medium, service, or record format in which the information is held. The same record may be stored within an integrated system containing information of different classification levels, provided that appropriate access controls are applied.4.1.3 Confidential Information

Confidential information is defined as information which is protected by Irish and/or EU legislation or regulations, HSE policies or legal agreements. It must be kept secure and only shared with people who are authorised to access it. The unauthorised or accidental disclosure of this information could adversely impact the HSE, its patients, its staff and its business partners. Some examples of confidential information include:

Patient / client / staff personal information (unless classified as restricted);
Patient /client / staff medical records (unless classified as restricted);
Patient appointment records;
PPS numbers and identifiers;
Staff personnel records;
Staff HR disciplinary records;
Unpublished medical research;
Financial information and budgetary reports;
Purchasing information;
Service plans and performance monitoring reports;
Draft reports;
Audit reports;

Incident reports
Vendor contracts / commercially sensitive information;
Information covered by non-disclosure / confidentiality agreements;
Security information e.g. passwords or encryption keys;
Information collected as part of criminal/HR investigations; and
Insurance and claims documentation.

4.1.4 Restricted Information

Restricted information is defined as highly sensitive confidential information. It is given a higher level of protection than confidential information. The unauthorised or accidental disclosure of this information would seriously and adversely impact the HSE, its patients, its staff and its business partners. Due to its sensitive nature, access should be limited to only those who have a clear business or clinical need to know. Some examples of restricted information include:

Information about a person's mental health status;
HIV status;
Sexually transmitted disease/infection (STD/STI) status;
Psychiatric assessments;
Sexual health clinic records;
Oncology treatment records;
Childcare / adoption records;
Social work records;
Child Protection and welfare records;
Addiction services information;
Disability services information;
Safeguarding investigation files;
Unpublished financial reports;
Strategic corporate plans;
Sensitive or unpublished medical research; and
Legal case files involving patients.

4.1.5 Note re Medical Record Types

The HSE manages many different types of medical and healthcare records. The following non-exhaustive list outlines common medical record types managed within the HSE:

Inpatient and outpatient clinical records;
Emergency department records;
Nursing notes and care plans;
Medication administration records (MAR);
Laboratory and diagnostic reports;
Radiology images and reports;
Theatre and procedure notes;
Mental health records;
Maternity and neonatal records;
Child protection and safeguarding records;
Social work records;
Occupational health records;
Community care records;
GP referral letters and discharge summaries;
Consent forms;
Incident and adverse event reports;
Clinical audit documentation;
Multidisciplinary team notes;
Telehealth / remote consultation records; and
Paper-based legacy archives and historical files.

All such records must be treated at a minimum as Confidential because they contain personal and healthcare information. All healthcare records containing personal health information shall be classified at a minimum as Confidential. Certain information within healthcare records may require classification as Restricted where unauthorised disclosure would be expected to result in significant harm to an individual, compromise the safety of a vulnerable person, or create substantial legal, clinical or reputational risk. Classification should be based on sensitivity and risk rather than clinical specialty alone (e.g. mental health, safeguarding, or sexual health). Staff must ensure these records are stored securely, only accessed by authorised people and handled according to HSE policies and procedures.

4.2 Information Classification Matrix

HSE Information Classification Matrix				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• Definition	• Information that is available to the general public and intended to be distributed outside the HSE. This information may be freely disseminated without potential harm.	• Information that is only intended to be distributed among HSE staff and authorised third parties (i.e. service providers, contractors/sub-contractors and agency staff).	• Information that is protected by Irish and/or EU legislation or regulations, HSE policies or legal contracts.	• Highly sensitive confidential information.
• Examples. The list of examples is for guidance and is not exhaustive.	• Patient/Client brochures • Staff brochures • News or media releases • Pamphlets • Advertisements • Web content • Job postings • Public Health Information	• Internal contact directory • Internally published policies and procedures • User manuals • Training manuals and documentation • Staff newsletters & magazines • Inter-office memorandums (depending on the content) • Business continuity plans	• Patient / client / staff personal information (except that which is restricted) • Patient / Client / Staff medical records (except that which is restricted) • Unpublished medical research • Staff personnel records • Financial information / budgetary reports • Service plans / service performance monitoring reports • Audit reports • Draft reports • Vendor contracts / commercially sensitive information • Information covered by non-disclosure / confidentiality agreements • Passwords / cryptographic private keys	• Patient / client / staff sensitive personal information (e.g. mental health status, HIV status, STD/STI status, etc.) • Childcare / Adoption information • Social Work information • Addiction services information • Disability services information • Unpublished financial reports • Strategic corporate plans; • Sensitive medical research

			• Incident reports; Information collected as part of criminal/HR investigations.	
• Possible consequences if information is mishandled	• None	• In the majority of instances, the unauthorised would not significantly impact the HSE, its staff, its patients, or clients.	• Unauthorised disclosure could adversely impact the HSE, its patients, its staff, its clients and its business partners.	• Unauthorised disclosure would seriously and adversely impact the HSE, its staff, its patients, its clients and its business partners.

4.3 Information Handling

All Information (irrespective of its format) owned, created, received, stored and processed by the HSE must be handled appropriately according to its classification.

These principles should be kept in mind when handling information.

1. Share or provide access to information on the basis of “need to know” and following the principle of “least privilege”.
2. Store HSE information assets in HSE-approved information systems and in a dedicated system of record for the information type, where available.
3. Records should be fit for purpose and available, with access control as appropriate to their sensitivity.
4. Maintain effective record keeping in line with HSE National Records Retention Policy through regular review and treatment of records.
5. Keep storage locations free of redundant, obsolete and trivial data through regular review and secure disposal.
6. Limit digital copies of information to minimise excess copies and securely dispose of excess copies immediately after use.
7. Drafts and working versions should be reviewed regularly. Where they do not constitute records requiring retention, they should be disposed of in accordance with approved information governance procedures. Where drafts contain evidence of significant decisions, approvals or development of policy, they may constitute records and should be retained in accordance with the applicable retention schedule.
8. Store only information under the control of HSE and keep storage locations free of third party or one’s own information.
9. The master record must be identified and stored in an approved system of record.
10. Duplicate, convenience and transitory copies should not be retained longer than operationally required.
11. Records subject to litigation, investigation, Freedom of Information requests, access requests, audits, inquiries or statutory holds must not be destroyed, regardless of retention schedule expiry, until the hold is formally lifted.
12. Records reaching the end of their retention period must undergo disposition review in accordance with NRRP requirements.

NB. **Information Handling Matrix** in Appendix One details how the different classifications of information must be handled.

5. Roles and Responsibilities

5.1 Information Owners

Information owners are responsible for the following.

- The implementation of this policy in keeping with all related information governance, information security, records management and data protection policies within the directorate, service or function under their control.
- Ensuring that all HSE information, irrespective of format, that are owned, created, received, stored or processed within their area of responsibility are appropriately classified, managed and handled in accordance with this policy.
- Ensuring appropriate governance arrangements, procedures and controls are in place to support compliance with information classification and handling
- Ensuring that all staff, students, contractors, sub-contractors, agency staff and third parties under their direction are made aware of, understand and comply with this policy and other relevant HSE policies.
- Ensuring that appropriate training, guidance and support are provided to promote ongoing compliance with this policy and other related HSE policies.

5.2 Line Managers

Line managers are responsible for:

- The implementation of this policy and all other relevant HSE policies within the business areas for which they are responsible;
- Ensuring all information (irrespective of its format) owned, created, received, stored and processed within the HSE business area they manage is classified and handled in line with this policy;
- Ensuring that all HSE staff, students, contractors, sub-contractors and agency staff who report to them are made aware of, understand and have access to this policy and all other relevant HSE policies;
- Ensuring that all HSE staff, students, contractors, sub-contractors and agency staff who report to them are instructed to comply with this policy and all other relevant HSE policies;

Ensuring that all HSE staff, students, contractors, sub-contractors and agency staff who report to them are provided with adequate information and training regarding the implementation of this policy and all other relevant HSE policies
Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

5.3 Staff

Each staff member is responsible for.

- Complying with the terms of this policy and all other relevant HSE policies, procedures, regulations and applicable legislation;
- Ensuring all information (irrespective of its format) for which they are responsible is classified and handled in line with this policy;
- Reporting all misuse and breaches of this policy to their line manager.

5.4 Contractors, Sub-contractors and Agency Staff

Each contractor, sub-contractor or agency staff member is responsible for:

- Complying with the terms of this policy and all other relevant HSE policies, procedures, regulations and applicable legislation;
- Ensuring all information (irrespective of its format) for which they are responsible is classified and handled in line with this policy; and
- Reporting all misuse and breaches of this policy to their contracted HSE line manager.

5.5 Third party commercial service providers

Third party commercial service providers are responsible for:

- Complying with the terms of this policy and all other relevant HSE policies, procedures, regulations and applicable legislation;
- Ensuring all information (irrespective of its format) for which they are responsible is classified and handled in line with this policy; and
- Reporting all misuse and breaches of this policy to their HSE contact.

6. Policy Governance and Implementation

6.1 Disclosure of interests

There are currently no conflicts of interest identified as yet pending review.

6.2 Methodology

This policy provides a framework for the classification and handling of HSE information assets and addresses the following key questions:

- What information assets are covered by this policy and why is information classification important?
- What are the HSE information classification levels and how is the appropriate classification determined?
- Who is responsible for classifying and handling HSE information?
- How should information be stored, accessed, used, shared and transferred according to its classification?
- What security controls are required to protect information from unauthorised access, disclosure, alteration, loss or destruction?
- When and how should information be securely disposed of in accordance with its classification and format?

6.3 Consultation and Review Process

The policy review process employed the following approach:

Planning: A cross-functional Stakeholder's Review Group was established accountable to the policy commissioner. A communication channel for employees and policy users was created, providing opportunities for queries, input and feedback.

Consultation, Gap Analysis and Assessment: During this step, areas for improvement were identified through query management, stakeholders' consultation and feedback collection. Feedback was considered and updates were made to this policy, where relevant.

Supporting Evidence: A search of similar and publicly available policies in other jurisdictions was undertaken to identify best practices and potential areas for

improvement. To ensure that this policy does not conflict with other or related documents, related policies which are available on the HSE National Central Repository were also noted.

Evaluation and Developing policy options: This step includes a range of potential actions to inform the proposed revisions. A series of engagements were undertaken to inform drafting of revisions to the policy.

Draft and Propose Revisions. Final draft is developed along with an audit checklist for implementation, and submitted to decision-making or relevant committees for approval, followed by circulation for a wider consultation.

- Formal approval, publication, communication and dissemination

6.4 National implementation plan

Managers at all levels are responsible for implementing this National Policy within their areas of responsibility. This includes identifying responsible persons, ensuring the implementation of appropriate local procedures and controls, and establishing suitable timeframes for implementation and ongoing compliance.

Public Involvement, Culture and Risk Management (PICRM), as the national policy owner, is responsible for the implementation, communication, maintenance and governance of this policy, including the provision of supporting guidance, tools and standards as required. Technology & Transformation will support services through the development of implementation resources, monitoring arrangements and compliance requirements.

Relevant services and business areas should, where appropriate, develop local Standard Operating Procedures (SOPs), work instructions or operational guidance to support implementation of this policy and translate its requirements into practical operational processes.

Refer to the National Implementation Plan (Appendix 4) and National Audit Tool (Appendix 5) for further guidance on implementation, monitoring and compliance with this policy.

6.5 Governance and approval

This policy has been developed through the National Records Management Programme working group. Following approval by the Group, it will be submitted to the Records management steering group committee for review and recommendation or otherwise.

If recommended for approval, it will be submitted to the SLT for approval. The SLT may choose to request final approval by the Board Audit and Risk Committee. Once approved, the final version was converted to a PDF document to ensure the integrity of the policy and uploaded to the HSE National Central Repository. A signed and dated copy of the checklist was attached to the master copy, which is retained with the office of the National Director Public Involvement, Culture and Risk Management (PICRM).

6.6 Monitoring and audit

The ongoing monitoring, audit and evaluation in the National Implementation Plan (Appendix II), aims to support the sustained implementation of the policy. Managers are required to monitor and audit the implementation of the Policy annually within their area of responsibility using the audit checklist (Appendix III) and maintain evidence of same. It is recommended that verification of compliance with this policy is included in local compliance monitoring activities on an annual basis.

6.7 Policy review and update

This policy will be reviewed on a 3 yearly basis unless there is any new supporting evidence identified by findings from audit and evaluation, advances in technology or research, then the policy should be reviewed, updated and published as necessary.

7. References

Information classification is part of an information security management system under the industry standard ISO/IEC 27001:2022 and is set out in the information security controls below.

> *Information should be classified according to the information security needs of the organisation based on confidentiality, integrity, availability and relevant interested party requirements.*

ISO/IEC 27001:2022 Annex A 5.12 Classification of Information

> *An appropriate set of procedures for information labelling should be developed and implemented in line with the information classification scheme adopted by the organisation.*

ISO/IEC 27001:2022 Annex A 5.13 Labelling of Information

> *Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organisation and between the organisation and other parties.*

ISO/IEC 27001:2022 Annex A 5.14 Information Transfer

> *An inventory of information and other associated assets, including owners, should be developed and maintained.*

ISO/IEC 27001:2022 Annex A 5.9 Inventory of information and other associated assets

These information security controls correspond to similar information asset management controls in other information security industry standards as set out in the table below.

ISO 27001:2022 Control	NIST CSF 2.0	COBIT 2019	SOC 2 (TSC)	CIS Controls v8	PCI DSS v4.0
A.5.9 Inventory of information and other associated assets	ID.AM-01, ID.AM-02 (Asset Management)	APO09.01, BAI09.01 (Manage Assets)	CC6.1 (Asset identification and classification)	CIS 1 (Inventory of Enterprise Assets), CIS 2 (Software Inventory)	Requirement 2.4, Requirement 12.3.3 (Maintain inventory of system components)
A.5.12 Classification of information	ID.AM-05 (Data classification & prioritization)	APO14.01 (Manage Data - Classification)	CC6.1, CC6.2 (Data lifecycle and protection categorization)	CIS 3.1 (Establish a Data Management Process)	Requirement 12.8.1 (Maintain a list of service providers & classification data)
A.5.13 Labelling of information	PR.DS-01 (Data-at-rest protection/label mechanisms)	APO14.02 (Data quality & tagging rules)	CC6.3 (Procedural boundaries and identification)	CIS 3.2 (Configure Data Access Control Lists)	Requirement 3.2 (Exclusions/labelling of sensitive cardholder data)

A.5.14 Information transfer	PR.DS-02 (Data-in-transit protection), PR.DS-10	APO14.05, BAI04.07 (Manage Availability/Data Exchange)	CC6.6, CC6.7 (Transmission integrity and perimeter boundaries)	CIS 3.10 (Encrypt Data in Transit), CIS 15 (Service Provider Management)	Requirement 4 (Encrypt cardholder data across open, public networks)

This policy should be read in conjunction with the following HSE policies.

HSE Data Protection Policy
HSE National Manual Handling and People Handling Policy
HSE National Records Retention Policy 2025-2028 (NRRP)
HSE Standard Operating Procedure for the Management of Telephone or Video Enabled Care Clinical Practice
HSE Standards and Recommended Practices for Healthcare Records Management v3.0 2011
HSE IT Security Policies applicable to all users of HSE information assets

- HSE Cellular Mobile Device Policy
- HSE Cyber Security Awareness Training Policy
- HSE Electronic Communications Policy
- HSE Encryption Policy
- HSE Equipment Sanitation & Disposal Policy
- HSE Gen AI Usage Policy
- HSE ICT Asset Management Policy
- HSE ICT Physical & Environmental Security Policy
- HSE Identity & Access Management Policy
- HSE Information Technology (I.T.) Security Policy
- HSE IT Acceptable Use Policy
- IT Security Exceptions Policy
- HSE IT Security Policy Glossary
- HSE Multi-Factor Authentication Policy
- HSE Network Security Policy
- HSE Password & Passcode Policy
- HSE Remote Access Policy
- HSE Software Policy
- HSE Web Filtering Policy Version

When handling information by information classification, HSE staff should consult HSE guidance and training on HSE website or HSE intranet sites including:

CISO (office of the Chief Information Security Officer)
Compliance Obligations Register
Data Protection (from office of the Data Protection Officer)
Digital for Care
M365 Centre of Excellence
National Records Management Programme (HSE department of Public Involvement, Culture and Risk Management)

8. Appendices

8.1. Appendix I: Information Handling Matrix

8.1.1 Information Classification & Handling Procedures: General Handling

9. Information Classification & Handling Procedures				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• Document Marking	• No marking is required.	• Add “HSE – Internal” in the centre footer of each page or stamp appropriately. • In Microsoft 365, classify the file as “Internal” using sensitivity labelling. (Sensitivity labelling will automatically apply the document marking in the footer in line with policy.)	• Mark the front page of all documents “HSE - Confidential” and add “HSE – Confidential” to the centre footer of each page or stamp appropriately. • In Microsoft 365, classify the file as “Confidential” using sensitivity labelling. (Sensitivity labelling will automatically apply the document marking in the footer in line with policy.)	• Mark the front page of all documents “HSE - Restricted” and add “HSE – Restricted” to the centre footer of each page or stamp appropriately. • In Microsoft 365, classify the file as “Restricted” using sensitivity labelling. Sensitivity labelling will automatically apply the document marking in the footer in line with policy.)
• Access to / disclosure of the information	• Available to the general public.	• Generally made available to all staff, contractors, sub-contractors, agency staff. • Permit access to authorised third parties (i.e. service providers etc) on a need-to-know basis.	• Confidential information must only be accessible on a need-to-know basis. • Confidential information must only be: -- Accessible to HSE staff who have a legitimate HSE business need to access the information or have been authorised to access the information by the designated HSE information owner; -- Released and disclosed to the general public in line with the relevant legislation or regulation (e.g. Freedom of	• Restricted information must only be accessible on a need-to-know basis. • Restricted information must only be: -- Accessible to HSE staff who have a legitimate HSE business need to access the information or have been authorised to access the information by the designated HSE information owner; -- Released and disclosed to the general public in line with the relevant legislation or regulation (e.g. Freedom of

9. Information Classification & Handling Procedures				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
			Information Act or Data Protection Act); -- Released and disclosed outside the organisation in line with the relevant legislation or regulation (e.g. Freedom of Information Act or Data Protection Act); and -- Processed (collected, hosted, disposed, etc.) by third party service providers who have a legal contract in place with the HSE to provide information management services and have signed a copy of the HSE Service Provider Data Processing Agreement.	Information Act or Data Protection Act); -- Released and disclosed outside the organisation in line with the relevant legislation or regulation (e.g. Freedom of Information Act or Data Protection Act); and -- Processed (collected, hosted, disposed, etc.) by third party service providers who have a legal contract in place with the HSE to provide information management services and have signed a copy of the HSE Service Provider Data Processing Agreement.
• Publication on the Intranet / Internet	• Ensure that publication is authorised before publishing Internal information on the HSE intranet and internet sites. • The line manager of the HSE section or service area	• Ensure that publication is authorised before publishing Internal information on the HSE intranet, and sites which are internally accessible only. • The line manager of the HSE section or service area who is responsible for the information authorises publication.	• Never publish, post or discuss Confidential information on internal or publicly accessible websites or social media applications including internal or publicly available sites or applications which are officially sanctioned by the HSE. • This requirement is in line with HSE Electronic Communications Policy.	• Never publish, post or discuss Restricted information on internal or publicly accessible websites or social media applications including internal or publicly available sites or applications which are officially sanctioned by the HSE. • This requirement is in line with HSE Electronic Communications Policy.

9. Information Classification & Handling Procedures				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
	who is responsible for the information authorises publication.			
• Breach of Confidentiality: -- Loss or theft of information -- Loss or theft of a computer device containing the information -- Actual or suspected unauthorised access -- Accidental disclosure	• Immediately report all suspect cyber security incidents to National Service Desk (NSD). • No special requirements.	• Immediately report all suspect cyber security incidents to National Service Desk (NSD). • Report and handle all personal data breaches, or suspected loss, theft or unauthorised disclosure of personal data, in line with the HSE Data Breach Process Guidelines and guidance from Office of the Data Protection Officer.	• Immediately report all suspect cyber security incidents to National Service Desk (NSD). • Report and handle all personal data breaches, or suspected loss, theft or unauthorised disclosure of personal data, in line with the HSE Data Breach Process Guidelines and guidance from Office of the Data Protection Officer.	• Immediately report all suspect cyber security incidents to National Service Desk (NSD). • Report and handle all information breaches involving the actual or suspected loss, theft in line with the HSE Data Protection Policy and guidance from Office of the Data Protection Officer.
• Backup & Recovery	• HSE information should be retained on the HSE network or approved cloud storage, and as such, backup and recovery will be managed centrally by Technology & Transformation	• HSE information should be retained on the HSE network or om approved cloud storage, and as such, backup and recovery are managed centrally by Technology & Transformation under IT policies and procedures.	• HSE information should be retained on the HSE network or on HSE approved cloud storage, and as such, backup and recovery is managed centrally by Technology & Transformation under IT policies and procedures.	• HSE information should be retained on the HSE network or on HSE approved cloud storage, and as such, backup and recovery is managed centrally by Technology & Transformation under IT policies and procedures.

9. Information Classification & Handling Procedures				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
	under IT policies and procedures.			
• Printing, Scanning & Photocopying	• Limit printing, scanning and photocopying of Public information to minimise excess copies. • Destroy excess copies immediately after use.	• Limit printing, scanning and photocopying of Internal information to minimise excess copies. • Locate printers, scanners and photocopiers within an area which is not accessible by the general public. • Destroy excess copies immediately after use.	• Limit printing, scanning and photocopying of Confidential information to only when absolutely necessary, to protect confidentiality and minimise excess copies. • Locate printers, scanners and photocopiers within an area which is not accessible by the general public. • Always ensure original documents and copies are removed from printing/scanning/photocopying machine as soon as possible. • Destroy excess copies immediately after use.	• Restrict printing, scanning and photocopying of Restricted information to only when absolutely necessary, to protect confidentiality and minimise excess copies. • Locate printers, scanners and photocopiers within an area which is not accessible by the general public. • Always ensure original documents and copies are removed from printing/scanning/photocopying machine as soon as possible. • Destroy excess copies immediately after use.

8.1.2 Records Retention – Defined Storage Locations

The storage location of a record does not determine its retention period. All records must be assigned the appropriate retention category as specified in the HSE National Records Retention Policy.

Records retained in Microsoft 365, SharePoint, Teams, OneDrive, file shares, business systems, physical storage facilities and contracted storage facilities remain subject to the applicable retention schedule and disposition requirements. Information owners and managers are responsible for ensuring that records are retained only as long as required and securely disposed of following approved disposition processes.

Records Retention – Permitted Storage Locations of Master Records				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• Dedicated systems of record contracted and approved by HSE (e.g. HR, Finance, Clinical records systems)	• Permitted for contracted and approved systems.	• Permitted for contracted and approved systems.	• Confidential information must only be stored in the dedicated system for the particular record type, where such a dedicated system is available. • Permitted for contracted and approved systems.	• Restricted information must only be stored in the dedicated system for the particular record type, where such a dedicated system is available. • Permitted for contracted and approved systems.
• Dedicated systems - Attend Anywhere	• Not applicable	• Not applicable	• Attend Anywhere is the approved application for video and audio meetings involving patient-facing communication (TeleHealth). • (Attend Anywhere does not record and store video and audio meetings.) • See Standard Operating Procedure for the Management of Telephone or Video Enabled Care Clinical Practice.	• Attend Anywhere is the approved application for video and audio meetings involving patient-facing communication (TeleHealth). • (Attend Anywhere does not record and store video and audio meetings.) • See Standard Operating Procedure for the Management of Telephone or Video Enabled Care Clinical Practice.

Records Retention – Permitted Storage Locations of Master Records				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• HSE Cloud: M365 Communication Site (Intranet Site)	• This is permitted as a storage location for the master published copy of a record classified as Public.	• This is permitted as a storage location for the master published copy of a record classified as Internal (e.g. an internal policy).	• Not permitted.	• Not permitted.
• HSE Cloud: M365 SharePoint / Teams Site	• This is permitted as a storage location for the master original or published copy of a record classified as Public.	• This is permitted as a storage location for the master original or internally published copy of a record classified as Internal.	• This is permitted as a storage location for a record classified as Confidential.	• This is permitted as a storage location for a record classified as Restricted.
• HSE Cloud: M365 OneDrive	• Not permitted for storage of the master copy of a Public information record.	• Not permitted for storage of the master copy of an Internal information record.	• This is permitted as a storage location for a master record classified as Confidential only by exception and where necessary to maintain confidentiality.	• This is permitted as a storage location for a master record classified as Restricted only by exception and where necessary to maintain confidentiality.
• HSE Cloud: M365 Teams Chat	• This is a storage location for Teams Chat messages only. • Teams Chat messages are deleted automatically after 30 days.	• This is a storage location for Teams Chat messages only. • Teams Chat messages are deleted automatically after 30 days.	• Confidential personal data is not permitted in Teams Chat. • This is a storage location for Teams Chat messages only. • Teams Chat messages are deleted automatically after 30 days.	• Restricted information is not permitted in Teams Chat. • This is a storage location for Teams Chat messages only. • Teams Chat messages are deleted automatically after 30 days.

Records Retention – Permitted Storage Locations of Master Records				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• HSE Cloud: M365 Teams Meetings	• This is a storage location for Teams Meetings Chat messages, Recordings and Transcripts only, which are deleted automatically after 30 days.	• This is a storage location for Teams Meetings Chat messages, Recordings and Transcripts only, which are deleted automatically after 30 days.	• Confidential patient-facing information is not permitted in Teams Meetings. • This is a storage location for Meetings Chat, Recordings and Transcripts only, which are deleted automatically after 30 days.	• Restricted patient-facing information is not permitted in Teams Meetings. • This is a storage location for Meetings Chat, Recordings and Transcripts only, which are deleted automatically after 30 days.
• HSE networked storage: on-premise servers – file-shares	• Permitted. • This is a storage location for active and inactive records.	• Permitted. • This is a storage location for active and inactive records.	• Permitted. • This is a storage location for active and inactive records.	• Permitted. • This is a storage location for active and inactive records.
• HSE network – on-premise servers – personal shares	• Not permitted for storage of the master copy of a Public information record.	• Not permitted for storage of the master copy of an Internal information record.	• This is permitted as a storage location for a master record classified as Confidential only by exception and where necessary to maintain confidentiality.	• This is permitted as a storage location for a master record classified as Restricted only by exception and where necessary to maintain confidentiality.
• HSE desktop or laptop computer - local storage	• Not permitted.	• Not permitted.	• Not permitted.	• Not permitted.
• HSE mobile electronic communications device including telephone or tablet computer – local storage	• Not permitted.	• Not permitted.	• Not permitted.	• Not permitted.

Records Retention – Permitted Storage Locations of Master Records				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• HSE removable storage media, such as, external/portable hard drive, USB Memory Stick, CD/DVD, tapes or floppy disks	• Not permitted.	• Not permitted.	• Not permitted.	• Not permitted.
• HSE rich media device, i.e. a photographic, video or audio recording device	• Not permitted – transfer files to authorised storage location once content is captured.	• Not permitted – transfer files to authorised storage location once content is captured.	• Not permitted – transfer files to authorised storage location once content is captured.	• Not permitted – transfer files to authorised storage location once content is captured.
• Staff personal devices (i.e. Where the device is the staff members personal property and is not owned or leased by the HSE)	• Not permitted.	• Not permitted.	• Not permitted.	• Not permitted.
• National Archives	• HSE Archive collections approved to send to National Archives	• HSE Archive collections approved to send to National Archives	• HSE Archive collections approved to send to National Archives	• HSE Archive collections approved to send to National Archives
• Third-party off-site storage of physical information assets (under contract to HSE)	• Permitted for inactive records on paper, microfiche/microfilm and analogue	• Permitted for inactive records on paper, microfiche/microfilm and analogue carriers (e.g. tape).	• Permitted for inactive records on paper, microfiche/microfilm and analogue carriers (e.g. tape).	• Permitted for inactive records on paper, microfiche/microfilm and analogue carriers (e.g. tape).

Records Retention – Permitted Storage Locations of Master Records				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
	carriers (e.g. tape).			
• Third-party off-site storage of on-premise servers (approved and under contract to HSE and connected to HSE network)	• Permitted.	• Permitted. subject to third party having successfully undergone a HSE cybersecurity / data protection review and having signed a copy of the HSE Service Provider Data Processing Agreement.	• Permitted, subject to third party having successfully undergone a HSE cybersecurity / data protection review and having signed a copy of the HSE Service Provider Data Processing Agreement	• Permitted, subject to third party having successfully undergone a HSE cybersecurity / data protection review and having signed a copy of the HSE Service Provider Data Processing Agreement.
• Third-party cloud storage (approved and under contract to HSE - e.g. HSE's tenant on Microsoft 365)	• Permitted.	• Permitted. subject to third party having successfully undergone a HSE cybersecurity / data protection review and having signed a copy of the HSE Service Provider Data Processing Agreement.	• Permitted. subject to third party having successfully undergone a HSE cybersecurity / data protection review and having signed a copy of the HSE Service Provider Data Processing Agreement.	• Permitted. subject to third party having successfully undergone a HSE cybersecurity / data protection review and having signed a copy of the HSE Service Provider Data Processing Agreement.
• HSE Exchange Email Mailboxes	• Mailboxes are a storage location for email records only and should not be treated as the primary repository for records requiring long-term retention. Email attachments are generally copies of a master record and should only	• Mailboxes are a storage location for email records only and should not be treated as the primary repository for records requiring long-term retention. Email attachments are generally copies of a master record and should only be retained within the mailbox where necessary as part of the email record. Where an email or its attachment	• Mailboxes are a storage location for email records only and should not be treated as the primary repository for records requiring long-term retention. Email attachments are generally copies of a master record and should only be retained within the mailbox where necessary as part of the email record. Where an email or its attachment	• Mailboxes are a storage location for email records only and should not be treated as the primary repository for records requiring long-term retention. Email attachments are generally copies of a master record and should only be retained within the mailbox where necessary as part of the email record. Where an email or its attachment

Records Retention – Permitted Storage Locations of Master Records				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
	be retained within the mailbox where necessary as part of the email record. Where an email or its attachment constitutes a business, legal, clinical, financial, HR, or administrative record, it must be captured into the appropriate approved system of record and retained in accordance with the applicable retention schedule. Retention of records within email mailboxes does not replace records management obligations under the HSE National Records Retention Policy. Email retention	constitutes a business, legal, clinical, financial, HR, or administrative record, it must be captured into the appropriate approved system of record and retained in accordance with the applicable retention schedule. Retention of records within email mailboxes does not replace records management obligations under the HSE National Records Retention Policy. Email retention settings do not replace records management obligations.	constitutes a business, legal, clinical, financial, HR, or administrative record, it must be captured into the appropriate approved system of record and retained in accordance with the applicable retention schedule. Retention of records within email mailboxes does not replace records management obligations under the HSE National Records Retention Policy. Email retention settings do not replace records management obligations. • To protect Confidential information, copy file attachments containing Confidential information to a secure folder to maintain as a master copy or secondary copy of a record and then delete the attachment from the email (for example, proof of identity such as a scanned image of a driver's licence).	constitutes a business, legal, clinical, financial, HR, or administrative record, it must be captured into the appropriate approved system of record and retained in accordance with the applicable retention schedule. Retention of records within email mailboxes does not replace records management obligations under the HSE National Records Retention Policy. Email retention settings do not replace records management obligations. • To protect Restricted information, copy file attachments containing Restricted information to a secure folder to maintain as a master copy or secondary copy of a record and then delete the attachment from the email.

Records Retention – Permitted Storage Locations of Master Records				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
	settings do not replace records management obligations.			

8.1.3 Storage of and Access to of Electronic-Based Information

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• HSE Website.	• Permitted.	• Prohibited.	• Prohibited.	• Prohibited.
• HSE Cloud: M365 Communication Site (Intranet Site)	• Apply the sensitivity label "Public" to the Communication Site to classify the information. • No special precautions on access are required.	• Apply the sensitivity label "Internal" to classify the information. • Only share internal information with HSE staff and authorised external users who have a 'need-to-know'; and remove external access when it is no longer required.	• Prohibited.	• Prohibited.
• HSE Cloud: M365 SharePoint / Teams Site	• Apply the sensitivity label "Public" to classify the information. • Public information may be stored in Teams Site / SharePoint but is	• Apply the sensitivity label "Internal" to classify the information. • Only share internal information with HSE staff and authorised external users who have a 'need-to-know'; and remove external	• Apply the sensitivity label "Confidential" to classify the information. • Only share confidential information with authorised users who have a 'need-to-know'.	• Apply the sensitivity label "Restricted" to classify the information. • Only share Restricted information with authorised users who have a 'need-to-know'.

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
	only accessible or shareable by link from Teams Site / SharePoint to HSE staff and authorised external users.	access when it is no longer required.	• Regularly review and remove access when it is no longer required.	• Regularly review and remove access when it is no longer required.
• HSE Cloud: M365 OneDrive	• Apply the sensitivity label "Public" to classify the information. • Public information may be stored in Teams Site / SharePoint but is only shareable by link from OneDrive to HSE staff and authorised external users.	• Apply the sensitivity label "Internal" to classify the information. • Only share a file containing internal information with HSE staff and authorised external users who have a 'need-to-know'; and remove external access when no longer required.	• Apply the sensitivity label "Confidential" to classify the information. • Store confidential information in OneDrive only by exception and if necessary to maintain confidentiality. • Only share confidential information with authorised users who have a 'need-to-know'. • Regularly review and remove access when it is no longer required.	• Apply the sensitivity label "Restricted" to classify the information. • Store restricted information in OneDrive only by exception and if necessary to maintain confidentiality. • Only share restricted information with authorised users who have a 'need-to-know'. • Regularly review and remove access when it is no longer required.
• HSE Cloud: M365 Teams Chat	• M365 Chat are restricted by invite only.	• Only share Internal information with HSE staff and authorised external users who have a 'need-to-know'. • Teams Chat messages are deleted automatically after 30 days.	• Prohibited. • Teams Chat messages are deleted automatically after 30 days.	• Prohibited. • Teams Chat messages are deleted automatically after 30 days.
• HSE Cloud: M365 Teams Meetings (Live Meeting,	• Ensure that publicly available M365 Meetings	• A Teams Meeting might be classified as "Internal" in	• Do not use Teams Meetings for patient-facing communication. Use Attend	• Do not use Teams Meetings for patient-facing communication. Use Attend

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Chat, Recording, Transcription)	contain only information which could be classified as Public.	certain contexts, such as training. • Consult M365 Information Management guidance for details on compliant management of Teams Meetings. • Teams Meetings recordings and transcripts automatically delete after 30 days when stored in their default location only.	Anywhere only. See Standard Operating Procedure for the Management of Telephone or Video Enabled Care Clinical Practice. • Limit invitations to users with a “need-to-know”. • Consult M365 Information Management guidance for details on compliant management of Teams Meetings. • . • Teams Meetings recordings and transcripts automatically delete after 30 days when stored in their default location only.	Anywhere only. See Standard Operating Procedure for the Management of Telephone or Video Enabled Care Clinical Practice. • Limit invitations to users with a “need-to-know”. • Consult M365 Information Management guidance and for details on compliant management of Teams Meetings. • Teams Meetings recordings and transcripts automatically delete after 30 days when stored in their default location only.
• HSE networked storage: on-premise servers – file-shares	• No special precautions required.	• Only share internal information with HSE staff and authorised external users who have a ‘need-to-know’; and remove external access when it is no longer required.	• Only share confidential information with authorised users who have a ‘need-to-know’. • Regularly review and remove access when it is no longer required.	• Only share restricted information with authorised users who have a ‘need-to-know’. • Regularly review and remove access when it is no longer required.
• HSE network – on-premise servers – personal shares	• No special precautions required.	• Only share internal information with HSE staff and authorised external users who have a ‘need-to-know’; and remove external access when it is no longer required.	• Only share confidential information with authorised users who have a ‘need-to-know’. • Regularly review and remove access when it is no longer required.	• Store restricted information in OneDrive only by exception and if necessary to maintain confidentiality. • Only share restricted information with authorised

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
				users who have a 'need-to-know'. • Regularly review and remove access when it is no longer required.
• HSE desktop or laptop computer – storage on local hard drive	• Storage of information on a local hard drive is not recommended.	• Storage of information on a local hard drive is not recommended.	• Strictly prohibited except where storage on a local drive is necessary for business or technical reasons temporarily or otherwise and, -- M365 or on-premise network server storage is not available to the user; or access to the network is temporarily unavailable; -- the computer is password protected in line with the HSE Password & Passcode Policy; -- the computer has been encrypted in line with the HSE Encryption Policy; and -- Information is backed up to the HSE cloud or on-premise network on a regular basis.	• Strictly prohibited except where storage in a private drive is necessary for business or technical reasons temporarily or otherwise and, -- OneDrive or a networked personal share is not available to the user; or access to the network is temporarily unavailable; -- the computer is password protected in line with the HSE Password & Passcode Policy; -- the computer has been encrypted in line with the HSE Encryption Policy; and -- Information is backed up to the HSE cloud or on-premise network on a regular basis.
• HSE mobile electronic communications device including telephone or	• Storage of information on a local hard drive is not recommended.	• Storage of information on a local hard drive is not recommended.	• Strictly prohibited except where storage on a local drive is necessary for business or technical reasons temporarily or otherwise and,	• Strictly prohibited except where storage on a local drive is necessary for business or technical

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
tablet computer – local storage			-- M365 or on-premise network server storage is not available to the user; or access to the network is temporarily unavailable; -- the mobile device is password protected in line with the HSE Password & Passcode Policy; -- the mobile device has been encrypted in line with the HSE Encryption Policy; and -- Information is backed up to the HSE cloud or on-premise network on a regular basis.	reasons temporarily or otherwise and, -- M365 or on-premise network server storage is not available to the user; or access to the network is temporarily unavailable; -- the mobile device is password protected in line with the HSE Password & Passcode Policy; -- the mobile device has been encrypted in line with the HSE Encryption Policy; and -- Information is backed up to the HSE cloud or on-premise network on a regular basis.
• HSE removable storage media, such as, external/portable hard drive, USB Memory Stick, CD/DVD, tapes or floppy disks	• Do not store information on removable media. • Consult Records Management Programme on the review and treatment of inactive records held on removable media. • Do not use removable media to transfer data	• Do not store information on removable media. • Consult Records Management Programme on the review and treatment of inactive records held on removable media. • Do not use removable media to transfer data (except for authorised exceptions) – use HSE-authorised secure file	• Strictly prohibited. • Do not store information on removable media. • Consult Records Management Programme on review and treatment of inactive records held on removable media. • Do not use removable media to transfer data (except for authorised exceptions) – use HSE-authorised secure file transfer (Citrix ShareFile) or email to transfer data.	• Strictly prohibited. • Do not store information on removable media. • Consult Records Management Programme on review and treatment of inactive records held on removable media. • Do not use removable media to transfer data (except for authorised exceptions) – use HSE-authorised secure file transfer (Citrix ShareFile) or email to transfer data.

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
	(except for authorised exceptions) – use HSE-authorised secure file transfer (Citrix ShareFile) or email to transfer data.	transfer (Citrix ShareFile) or email to transfer data.		
• HSE rich media device, i.e. a photographic, video or audio recording device	• Do not store HSE information on a rich media device. Copy the data to HSE cloud or HSE networked server once captured and delete the data from the device after transfer. • Consult Records Management Programme on review and treatment of inactive records held on rich media devices.	• Do not store HSE information on a rich media device. Copy the data to HSE cloud or HSE networked server once captured and delete the data from the device after transfer. • Consult Records Management Programme on review and treatment of inactive records held on rich media devices.	• Do not store HSE information on a rich media device. Copy the data to HSE cloud or HSE networked server once captured and delete the data from the device after transfer. • In the event that this cannot be carried out immediately the photographic or video recording device should be locked away securely when not in use. • Consult Records Management Programme on review and treatment of inactive records held on rich media devices.	• Do not store HSE information on a rich media device. Copy the data to HSE cloud or HSE networked server once captured and delete the data from the device after transfer. • In the event that this cannot be carried out immediately the photographic or video recording device should be locked away securely when not in use. • Consult Records Management Programme on review and treatment of inactive records held on rich media devices.
• Staff personal devices (i.e. Where the device is the staff	• Do not store HSE information on a personal device.	• Do not store HSE information on a personal device.	• Strictly prohibited.	• Strictly prohibited.

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
members personal property and is not owned or leased by the HSE)				
• Third party cloud or off-site storage (i.e. where the storage of the information has been outsourced to a third-party company)	• Store HSE Internal information on third-party cloud or off-site storage only under HSE Standard Terms for ICT Supplies and Services (or equivalent), which includes intellectual property terms.	• Store HSE Internal information on third-party cloud or off-site storage only under HSE Standard Terms for ICT Supplies and Services (or equivalent), which includes confidentiality terms.	• Store HSE Confidential information on third-party cloud or off-site storage only under HSE Standard Terms for ICT Supplies and Services (or equivalent), which includes confidentiality terms. • Do not store HSE Confidential information on third-party cloud or off-site storage where there are no contract terms, temporarily or otherwise. (If access is necessary pre-contract, consider approved guest access to HSE M365.)	• Store HSE Restricted information on third-party cloud or off-site storage only under HSE Standard Terms for ICT Supplies and Services (or equivalent), which includes confidentiality terms. • Do not store HSE Restricted information on third-party cloud or off-site storage where there are no contract terms, temporarily or otherwise. (If access is necessary pre-contract, consider approved guest access to HSE M365.)
• HSE Exchange Email Mailboxes	• Apply the sensitivity label “Public” to classify an outgoing email before sending. • Categorize incoming emails containing Public information with	• Apply the sensitivity label “Internal” to classify an outgoing email before sending. • Categorize incoming emails containing Internal information with the category “Internal”.	• Apply the sensitivity label “Confidential” to classify an outgoing email before sending. • Categorize incoming emails containing Confidential information with the category “Confidential”. • To protect Confidential information, copy file	• Apply the sensitivity label “Restricted” to classify an outgoing email before sending. • Categorize incoming emails containing Restricted information with the category “Restricted”. • To protect Restricted information, copy file

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
	the category "Public".		attachments containing Confidential information to a secure folder to maintain as a master copy or secondary copy of a record and then delete the attachment from the email (for example, proof of identity such as a scanned image of a driver's licence). • Save an email as a PDF if it is necessary to store a copy in a secure folder for business purposes.	attachments containing Restricted information to a secure folder to maintain as a master copy or secondary copy of a record and then delete the attachment from the email (for example, proof of identity such as a scanned image of a driver's licence). Save an email as a PDF if it is necessary to store a copy in a secure folder for business purposes.

8.1.4 Storage of Paper & Film Based Information

Information Classification & Handling Procedures				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• Paper documents and other printed material	• No special precautions to protect sensitivity required. • Reasonable precautions to prevent the risk of deterioration and loss of HSE records.	• Reasonable precautions to prevent the risk of deterioration, loss and access by unauthorised third parties.	• The information must be stored in such a way so as to ensure it is protected against the following. -- Unauthorised access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. -- Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc). -- Deterioration and/or loss.	• The information must be stored in such a way so as to ensure it is protected against the following. -- Unauthorised access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. -- Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc). -- Deterioration and/or loss.

• Microfilm, Microfiche and other image photo negative materials	• No special precautions to protect sensitivity required. • Reasonable precautions to prevent the risk of deterioration and loss of HSE records.	• Reasonable precautions to prevent the risk of deterioration, loss and access by unauthorised third parties.	• The information must be stored in such a way so as to ensure it is protected against the following. -- Unauthorised access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. -- Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc). -- Deterioration and/or loss.	• The information must be stored in such a way so as to ensure it is protected against the following. -- Unauthorised access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. -- Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc). -- Deterioration and/or loss.

8.1.5 Transfer, disclosure and sharing of information: spoken word and post

Transfer, disclosure and sharing of information: spoken word and post				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• Spoken word, such as, informal conversations, meetings or phone calls	• No special precautions required.	• No special precautions required.	• Confidential information should only be discussed with authorised individuals within a private setting. • Avoid discussion in public areas such as elevators, hallways, staircases and cafeterias, etc. • If you have to discuss a matter on the telephone, ensure you can positively identify the person you are talking to.	• Restricted information should only be discussed with authorised individuals within a private setting. • Avoid discussion in public areas such as elevators, hallways, staircases and cafeterias, etc. • If you have to discuss a matter on the telephone, ensure you can positively identify the person you are talking to.
• Internal Post	• Email or secure file transfer is preferable to internal post where feasible. • No special handling required.	• Email or secure file transfer is preferable to internal post where feasible. • No special handling required.	• Email or secure file transfer is preferable to internal post where feasible. • Follow standard internal postal procedure. • Notify the recipient in advance if feasible. • Check that you have the correct name and address of the intended recipient on the envelope. • Send in a sealed inter-office envelope marked “HSE - Confidential”. • Where sending information by removable storage media is an authorised exception, encrypt all removable storage media containing Confidential information in line with the HSE	• Email or secure file transfer is preferable to internal post where feasible. • Follow standard internal postal procedure. • Notify the recipient in advance if feasible. • Check that you have the correct name and address of the intended recipient on the envelope. • Send in a sealed inter-office envelope marked “HSE - Restricted”. • Where sending information by removable storage media is an authorised exception, encrypt all removable storage media containing Restricted information in line with the HSE Encryption Policy prior to being sent in the post. The data should be

			Encryption Policy prior to being sent in the post. • Securely dispose of information on removable storage media once transfer is complete. The data should be sanitised from the medium so that it is irrecoverable.	sanitised from the medium so that it is irrecoverable.
• External Post	• Check that you have the correct name and address of the intended recipient on the envelope.	• Check that you have the correct name and address of the intended recipient on the envelope. • Only send Internal information externally when a third-party organisation or individual has a need-to-know.	• Email or secure file transfer is preferable to external post for business-to-business communication where feasible. • Follow standard external postal procedure. • Notify the recipient in advance if feasible. • Check that you have the correct name and address of the intended recipient on the envelope. • Send in a sealed envelope marked “HSE - Confidential”. • Where sending information by removable storage media is an authorised exception, encrypt all removable storage media containing Confidential information in line with the HSE Encryption Policy prior to being sent in the post. • Bulk postal procedure. When sending bulk Confidential information by post to the same address you must use an approved courier or a registered postal service.	• Email or secure file transfer is preferable to external post for business-to-business communication where feasible. • Follow standard external postal procedure. • Notify the recipient in advance if feasible. • Check that you have the correct name and address of the intended recipient on the envelope. • Send in a sealed inter-office envelope marked “HSE -- Restricted”. • Where sending information by removable storage media is an authorised exception, encrypt all removable storage media containing Restricted information in line with the prior to being sent in the post. • Bulk postal procedure. When sending bulk Restricted information by post to the same address you must use an approved courier or a registered postal service.

8.1.6 Transfer, disclosure and sharing of information: electronic means

Transmission of Information: Electronic Transfer and Data Sharing				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• HSE Cloud: M365 Communication Site (Intranet Site)	• It is permitted to share public information by link to HSE staff and authorised third parties from a M365 Communication Site. • (M365 Communication Sites are not publicly accessible.)	• It is permitted to share Internal information by link to HSE staff and authorised third parties, based on a need-to-know from a M365 Communication Site.	• Not applicable.	• Not applicable.
• HSE Cloud: M365 SharePoint / Teams Site – Teams Site membership	• It is permitted to provide access to public information to HSE staff or authorised third parties as members of a Team's Site containing Public information only. • Regularly review the Teams Site content to monitor any change of information class	• It is permitted to provide access to Internal information to HSE staff or authorised third parties based on need-to-know as Teams Site members. • Regularly review the Teams Site content to monitor any change of information class and manage	• Only provide access to Confidential information as Teams Site members to authorised users based on 'need-to-know'. • Regularly review information class and Teams Site membership and remove access when it is no longer required.	• Only provide access to Restricted information as Teams Site members to authorised users based on 'need-to-know'. • Regularly review information class and Teams Site membership and remove access when it is no longer required. • Ensure that the number of Teams Site members is appropriately restricted.

Transmission of Information: Electronic Transfer and Data Sharing				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
	and manage access appropriate to the class.	access appropriate to the class. • Remove third party access when it is no longer required.		
• HSE Cloud: M365 SharePoint / Teams Site – link sharing	• It is permitted to share Public information by link to HSE staff and authorised third parties in a M365 SharePoint / Teams Site. • (M365 SharePoint / Teams Site are not publicly accessible.)	• It is permitted to share Internal information by link to HSE staff and authorised third parties based on a need-to-know from a M365 SharePoint / Teams Site. • Remove third party access when it is no longer required.	• Strictly limit sharing Confidential information by link. • Only share Confidential information by link with authorised users who have a 'need-to-know'. • Limit access permissions based on the principle of "least privilege" – e.g. limit to "view but no download" unless necessary to provide "view" or "edit" permissions. • Regularly review and remove access when it is no longer required.	• Strictly limit sharing Restrict information by link. • Limit sharing Restricted information by link with authorised users who have a 'need-to-know'. • Limit access permissions based on the principle of 'least privilege' – e.g. limit to "view but no download" unless necessary to provide "view" or "edit" permissions. • Regularly review and remove access when it is no longer required.
• HSE Cloud: M365 OneDrive – link sharing	• It is permitted to share Public information by link to HSE staff and authorised third parties in M365 OneDrive. • (M365 SharePoint / Teams Site are not publicly accessible.)	• It is permitted to share Internal information by link to HSE staff and authorised third parties based on a need-to-know from M365 OneDrive. • Remove third party access when it is no longer required.	• Only share Confidential information by link with authorised users who have a 'need-to-know'. • Limit access permissions based on the principle of "least privilege" – e.g. limit to "view but no download" unless necessary to provide "view" or "edit" permissions.	• Strictly limit sharing Restricted information by link with authorised users who have a 'need-to-know'. • Limit access permissions based on the principle of 'least privilege' – e.g. limit to "view but no download" unless necessary to provide "view" or "edit" permissions.

Transmission of Information: Electronic Transfer and Data Sharing				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
			• Regularly review and remove access when it is no longer required.	• Regularly review and remove access when it is no longer required.
• Secure file transfer service approved and contracted by HSE (Citrix ShareFile)	• It is permitted to transfer Public information by secure file transfer using HSE's approved secure file transfer application, Citrix ShareFile.	• It is permitted to transfer Internal information externally by secure file transfer using HSE's approved secure file transfer application, Citrix ShareFile, where a third-party organisation or individual has a "need to know".	• It is permitted to transfer Confidential information externally by secure file transfer using HSE's approved secure file transfer application, Citrix ShareFile. • Only transfer HSE Confidential information externally where it is necessary, a third-party organisation or individual has a "need to know", data protection and confidentiality agreement terms are in place, and remote access to HSE data environment was not feasible or appropriate to the purpose.	• It is permitted to transfer Restricted information by secure file transfer using HSE's approved secure file transfer application, Citrix ShareFile. • Only transfer HSE Restricted information externally where it is necessary, a third-party organisation or individual has a "need to know", data protection and confidentiality agreement terms are in place, and remote access to HSE data environment was not feasible or appropriate to the purpose.
• HSE networked storage: on-premise servers – file-shares	• Access to information in an on-premise file-share is managed solely through authorised read or read/write access to the file-share, which is administered by Technology & Transformation (raise ticket with	• Access to information in an on-premise file-share is managed solely through authorised read or read/write access to the file-share, which is administered by Technology & Transformation (raise ticket with	• Access to information in an on-premise file-share is managed solely through authorised read or read/write access to the file-share, which is administered by Technology & Transformation (raise ticket with National Service Desk for T&T support). Only users with HSE domain accounts may be authorised access. • Only provide access to Confidential information to	• Access to information in an on-premise file-share is managed solely through authorised access to the file-share read or read/write, which is administered by Technology & Transformation (raise ticket with National Service Desk for T&T support). Only users with HSE domain accounts may be authorised access. • Strictly, only provide access to Restricted information to

Transmission of Information: Electronic Transfer and Data Sharing				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
	National Service Desk for T&T support). • Only users with HSE domain accounts may be authorised access.	National Service Desk for T&T support). Only users with HSE domain accounts may be authorised access. • Raise ticket with NSD for T&T to remove access when it is no longer required.	authorised users who have a 'need-to-know'. • Regularly review and raise ticket with NSD for T&T to remove access when it is no longer required.	authorised users who have a 'need-to-know'. • Regularly review and raise ticket with NSD for T&T to remove access when it is no longer required.
• HSE network – on-premise servers – personal shares	• Access to information in a personal share is solely by access to the personal share itself. • Access should be authorised through line management and administered by Technology & Transformation for exceptional circumstances only.	• Access to information in a personal share is solely by access to the personal share itself. • Access should be authorised through line management and administered by Technology & Transformation for exceptional circumstances only.	• Access to information in a personal share is solely by access to the personal share itself. • Access should be authorised through line management and administered by Technology & Transformation for exceptional circumstances only. • Regularly review and remove access when it is no longer required.	• Access to information in a personal share is solely by access to the personal share itself. • Access should be authorised through line management and administered by Technology & Transformation for exceptional circumstances only. • Regularly review and remove access when it is no longer required.
• Sharing extracts of information – e.g. screenshot, in a presentation,	• Disclose or share extracts of information based on its sensitivity	• Disclose or share extracts of information based on its sensitivity	• Disclose or share extracts of information strictly based on its sensitivity level and "need-to-know" in the given context.	• Disclose or share extracts of information strictly based on its sensitivity level and "need-to-know" in the given context.

Transmission of Information: Electronic Transfer and Data Sharing				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
sharing a monitor screen.	level and "need-to-know".	level and "need-to-know".	• Redact, remove or anonymise any Confidential information if the recipient does not have a "need-to-know" or does not have a "need-to-know" in the context where the extract is being disclosed.	• Redact, remove or anonymise any Restricted information if the recipient does not have a "need-to-know" or does not have a "need-to-know" in the context where the extract is being disclosed.
• Internal Email (i.e. to an email address ending in @hse.ie)	• Apply the sensitivity label "Public" to the email to classify the information.	• Apply the sensitivity label "Internal" to the email to classify the information. • Email Internal information by link to HSE staff and authorised third parties based on a need-to-know only.	• Apply the sensitivity label "Confidential" to the email to classify the information. • Only email Confidential information to authorised users who have a 'need-to-know'. • Double check that the email address of the intended recipient is correct. • Write "Private & Confidential" in the subject heading. • Minimise the amount of sensitive information communicated in the email solely to what is necessary and proportionate to fulfil the purpose of the communication. • Sharing a link to (or attaching a password-protected file) Confidential information is recommended over including Confidential information in the body of the email.	• Apply the sensitivity label "Restricted" to the email to classify the information. • Only email Restricted information to authorised users who have a 'need-to-know'. • Double check that the email address of the intended recipient is correct. • Write "Strictly Private & Confidential" in the subject heading. • Minimise the amount of sensitive information communicated in the email solely to what is necessary and proportionate to fulfil the purpose of the communication. • Sharing a link to Restricted information (or attaching a password-protected file) is recommended over including Restricted information in the body of the email.

Transmission of Information: Electronic Transfer and Data Sharing				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• External Email (i.e. to an email address not ending in @hse.ie)	• Apply the sensitivity label "Public" to the email to classify the information. • BCC recipient email addresses of recipients if it is not necessary or relevant for a recipient to see other recipients' email addresses.	• Apply the sensitivity label "Internal" to the email to classify the information. • Email Internal information to authorised third parties based on a need-to-know only. • BCC recipient email addresses if recipients if it is not necessary or relevant for a recipient to see other recipients' email addresses.	• Apply the sensitivity label "Confidential" to the email to classify the information. • Only email confidential information with authorised recipients who have a 'need-to-know'. • Double check that the email address of the intended recipient is correct. • Write "Private & Confidential" in the subject heading. • Minimise the amount of sensitive information communicated in the email solely to what is necessary and proportionate to fulfil the purpose of the communication. • Sharing a link to Confidential information (or attaching a password-protected file) is recommended over including Confidential information in the body of the email. • BCC recipient email addresses if recipients if it is not necessary or relevant for a recipient to see other recipients' email addresses. • HSE email automatically includes a disclaimer in the email message.	• Apply the sensitivity label "Restricted" to the email to classify the information. • Only email Restricted information with authorised recipients who have a 'need-to-know' and, for personal data, where there is a legal basis under data protection legislation. • Double check that the email address of the intended recipient is correct. • Write "Private & Confidential" in the subject heading. • Minimise the amount of sensitive information communicated in the email solely to what is necessary and proportionate to fulfil the purpose of the communication. • Sharing a link (or attaching a password-protected file) to Restricted information is recommended over including Restricted information in the body of the email. • HSE email automatically includes a disclaimer in the email message. • All Restricted information included with the email message is encrypted in line with the HSE Encryption Policy unless the

Transmission of Information: Electronic Transfer and Data Sharing				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
				intended recipient email address is hosted on a network which connected to the HSE via a secure connection (for example: VPN, TLS connection etc).
• Health mail	• Not applicable.	• Not applicable.	• Use Healthmail to send Confidential clinical information.	• Use Healthmail to send Restricted clinical information.
• Text Message	• No special handling required	• No special handling required	• Prohibited with the limited exception below. • Under no circumstances whatsoever should Confidential information be transmitted by text. However, patients and service users who provide the HSE with prior explicit consent may be reminded by text message of their HSE appointments. Where patients and service users have consented to be contacted by text of their appointments, the text message should only contain the minimum amount of information, for example, the appointment date, time and the name of hospital. The specific HSE clinic the patient or service user is to attend may also be included in the text where this will not compromise privacy. The text message should not contain any personal information	• Prohibited.

Transmission of Information: Electronic Transfer and Data Sharing				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
			belonging to the patient or service user.	
• HSE Health App	• Communicate using HSE Health App to complement other communication media as directed by HSE guidelines and as appropriate to the sensitivity class of the information.	• Communicate using HSE Health App to complement other communication media as directed by HSE guidelines and as appropriate to the sensitivity class of the information.	• Communicate using HSE Health App to complement other communication media as directed by HSE guidelines and as appropriate to the sensitivity class of the information.	• Communicate using HSE Health App to complement other communication media as directed by HSE guidelines and as appropriate to the sensitivity class of the information.
• Telehealth	• Not applicable	• Not applicable	• See Standard Operating Procedure for the Management of Telephone or Video Enabled Care Clinical Practice.	• Standard Operating Procedure for the Management of Telephone or Video Enabled Care Clinical Practice.
• Fax	• Transfer by email or secure file transfer instead of fax. • For documents containing handwritten content, scan and email rather than fax.	• Transfer by email or secure file transfer instead of fax. • For documents containing handwritten content, scan and email rather than fax.	• Fax transmission has security vulnerabilities and is therefore not a recommended transmission medium at HSE for Confidential information. • Transfer by email or secure file transfer instead of fax. • For documents containing handwritten content, scan and email rather than fax. • If necessary to send by fax, confirm that the recipient is ready to receive the fax and only send to a fax machine kept in a	• Fax transmission has security vulnerabilities and is therefore not a recommended transmission medium at HSE for Restricted information. • Transfer by email or secure file transfer instead of fax. • For documents containing handwritten content, scan and email rather than fax. • If necessary to send by fax, confirm that the recipient is ready to receive the fax and only send to a fax machine kept in a

Transmission of Information: Electronic Transfer and Data Sharing				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
			restricted location. Once sent, confirm with the recipient that they received the fax.	restricted location. HSE email automatically includes a disclaimer in the email message.
• Consumer social media and other consumer communication applications, e.g. WhatsApp	▪ Consumer social media and communications applications are not approved to communicate HSE information except for an authorised HSE media campaign to the public communicated across consumer media.	▪ Consumer social media communications apps are not approved to communicate HSE information.	▪ Prohibited. ▪ Consumer social media communications apps are not approved to communicate HSE information.	▪ Strictly prohibited. ▪ Consumer social media communications apps are not approved to communicate HSE information.

8.1.7 Physical Security

Physical Security				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• Office / Workplace	• No special precautions required.	• No special precautions required.	• Restrict access to areas containing Confidential information based on "need-to-know" of staff members and authorised third parties. Restricted access could be controlled, for example, by an attended reception desk or a locked door accessible only by key, keypad or swipe card. • Regularly review access to restricted areas and revoke where there is no longer a "need-to-know" basis.	• Restrict access to areas containing Restricted information based on "need-to-know" of staff members and authorised third parties. Restricted access could be controlled, for example, by an attended reception desk or a locked door accessible only by key, keypad or swipe card. • Regularly review access to restricted areas and revoke where there is no longer a "need-to-know" basis.
• Laptop and desktop computer devices	• Laptop and desktop computers must be: -- Password protected in line with the HSE Password & Passcode Policy; -- Encrypted in line with HSE Encryption Policy -- Logged off or "locked" (using Ctrl+Alt+Delete keys) when they have to be left unattended for any period of time and at the end of each working day; and -- Regularly updated. • Passwords must not be written down on or near the device. • The device must be positioned in such a way as to minimise the risk of unauthorised individuals accessing the computer. • Laptops must be locked with a laptop cable lock or stored in a locked drawer or cabinet if left in the office overnight. • Laptops must be kept with you at all times when commuting or working off-site. • When working from home, laptops should be protected in the same manner as at the office. • Raise a ticket with National Service Desk to arrange for Technology & Transformation to take unassigned ("ownerless") and inaccessible computers.			

Physical Security				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
• HSE mobile electronic communications device including telephone or tablet computer	• Mobile devices must be: -- Password protected in line with the HSE Password & Passcode Policy; -- Locked when they have to be left unattended for any period of time and at the end of each working day; and -- Regularly updated. • Passwords must not be written down on or in an easily accessible location. • The device must be positioned in such a way as to minimise the risk of unauthorised individuals accessing the device. • Devices must be stored in a locked drawer or cabinet if not on the person. • Devices must be kept with you at all times when commuting or working off-site. • Raise a ticket with National Service Desk to arrange for Technology & Transformation to take unassigned ("ownerless") and inaccessible mobile devices.			
• HSE removable storage media, such as, external/portable hard drive, USB Memory Stick, CD/DVD, tapes or floppy disks	• Do not store information on removable media or use removable media to transfer information. • Use only encrypted removable media provided by Technology & Transformation by authorised exception, if necessary, by exception only, to transfer information using removable media. • Do not connect removable media to a HSE device except as authorised by Technology & Transformation. • If you find removable media, contact the National Service Desk for Technology & Transformation to support examining the contents. • Securely dispose of removable media once any HSE records are transferred. Contact National Service Desk to arrange for Technology & Transformation to manage secure disposal. • Consult Records Management Programme on the review and treatment of inactive records held on removable media (once NSA has confirmed if you can connect to the media). • If it is necessary to store information on a legacy carrier by exception (e.g. analogue removable media), store in a locked, fireproof cabinet or in authorised offsite storage.			
• Photographic, Video & • Audio Recording Devices	• Store in a secure location such as a locked filing cabinet, drawer or a safe when not in use. • Transfer all information from the device to an approved storage location before storing the device.			

8.1.8 Destruction & Disposal of Information

Secure disposal of information

1. Any decision to destroy and dispose of HSE information (irrespective of format) should be made in line with HSE National Records Retention Policy and the HSE National Hospital Office Code of Practice for Healthcare Records Management – Part 5: Retention and Disposal Schedule.
2. Prior to destruction, records identified as potentially possessing historical, cultural, evidential or research value must be reviewed in accordance with National Records Management Programme guidance. Records determined to have enduring archival value should be transferred to the National Archives of Ireland in accordance with applicable legislation and HSE archival procedures (refer to Guidance on Historical Records that may be of Archival value V1).
3. Consult industry standards on sanitising data so that it is irrecoverable: NIST Special Publication 800-88: Guidelines for Media Sanitation and also, IEEE P2883 and ISO/IED 21964.
4. Records may only be destroyed following:

- Verification that the approved retention period has expired;
- Completion of a documented disposition review;
- Confirmation that no litigation hold, investigation, inquiry, audit requirement, FOI request, access request or statutory restriction applies;
- Approval in accordance with the HSE National Records Retention Policy and local records management procedures.
- Records destruction activities must be documented and auditable.

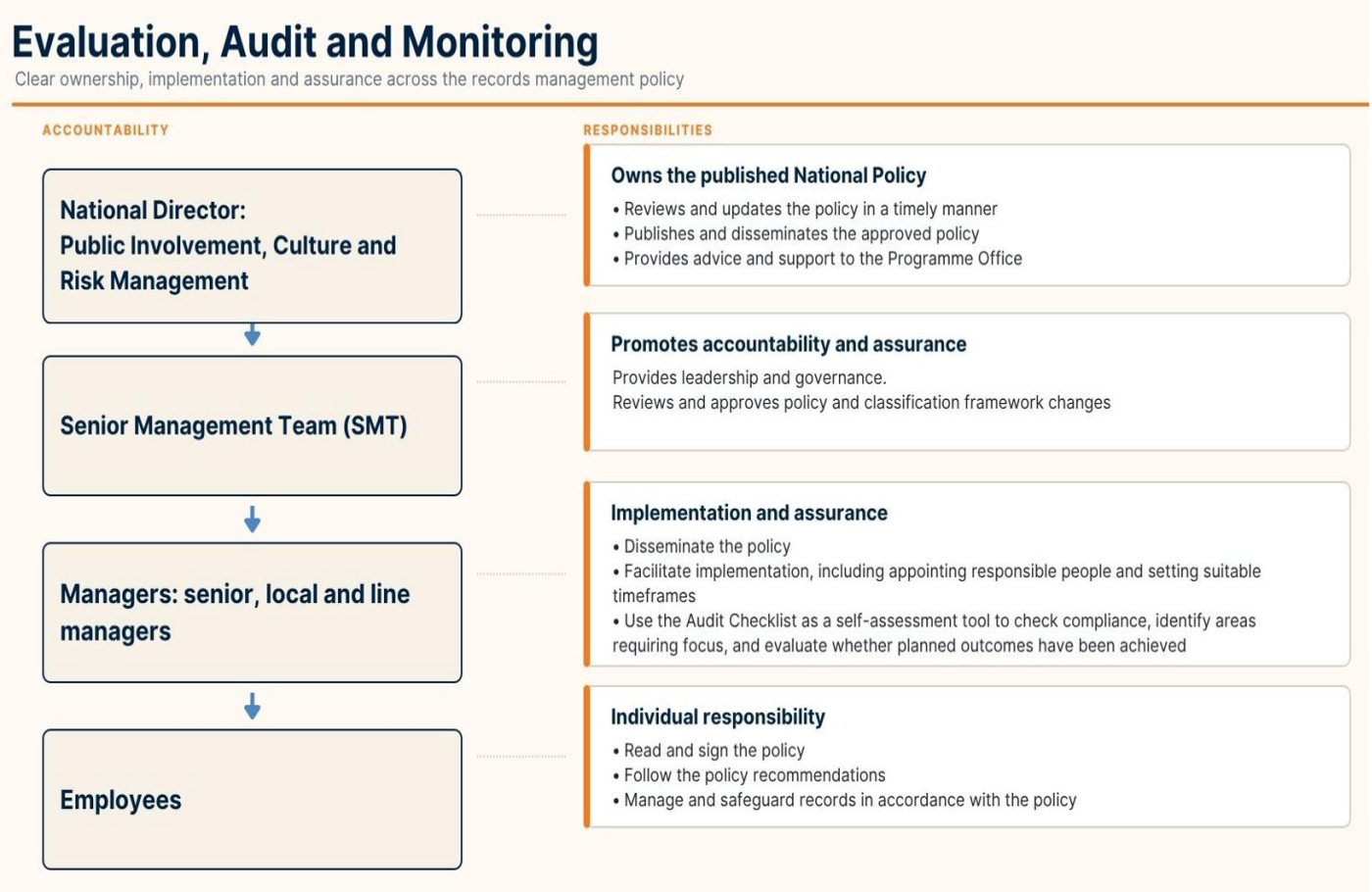
Topic	▪ Public	▪ Internal	▪ Confidential	▪ Restricted
• Paper & Film based information including paper records & printed material, microfilm, micro fiche and photographic materials	• Dispose of with general waste or shred at least at P-1 level.	• Securely dispose of by shredding at least P-2 level. • Consult Records Management Programme guidance on the secure disposal of paper and film records.	• Securely dispose of by shredding at least at P-3 level. • Secure disposal should only be carried out onsite or by a HSE contracted and approved third party supplier, and the service provider should provide a certification of destruction to the HSE department commissioning the secure disposal.	• Securely dispose of by shredding at least at P-3 level. • Where the destruction and disposal of the confidential information is outsourced to a third party service provider, the third party service provider must sign the HSE Service Provider Confidentiality Agreement. • Provide the subscribing HSE department with a

			• Consult Records Management Programme guidance on the secure disposal of paper and film records.	certificate of information destruction / disposal.
• End user hardware including desktop and laptop devices; mobile electronic communications devices; rich media devices (still image, video, audio); removable media; and photocopiers, scanners and fax machines.	• If the device is accessible, clear the device of information before sending for secure disposal. • Contact National Service Desk to arrange for Technology & Transformation to: -- securely dispose of data to industry standard and so that it is irrecoverable -- send to the authorised supplier of secure disposal services -- confirm secure disposal of the device and retain a certificate of destruction from the supplier. • The authorised supplier should carry out secure disposal in line with industry standards on security and in compliance with environmental regulations. • The supplier should provide a certificate of destruction, which is held by the Technology & Transformation. (Certificates of destruction of all electronic devices and media should be held by Technology & Transformation.) • Only Technology & Transformation may authorise and oversee recycling of hardware.			
Method of secure disposal and sanitisation Note: each media type requires its own method to sanitise the data so that it is irrecoverable. Refer to NIST Special Publication 800-88: Guidelines for Media Sanitation for industry standard methods.				
• Paper, microfiche and microfilm	• Shred, pulverise, macerate or incinerate. • Shred at the level appropriate to the information classification.			
• Photocopiers, Scanners and Fax Machines	• Most multifunctional photocopiers and scanners contain a hard disk which stores a copy of every document that was ever copied, scanned or faxed on the device. For this reason, old and end of life photocopiers must have their hard disk physically destroyed to ensure any confidential information cannot be recovered from the hard drive.			
• CDs/DVDs	• Shred, use sandpaper or incinerate.			
• Magnetic disks	• Degausse, pulverise or incinerate.			
• Video & audio tapes	• Pulverise or incinerate.			
• Electronic data	• HSE electronic information systems must sanitise electronic records using the applicable method recommended by the industry standard, NIST Special Publication 800-88: Guidelines for Media Sanitation.			

	• HSE staff should delete electronic data when it is no longer required and in compliance with HSE National Records Retention Policy. The staff member should double check that data has been successfully deleted and carry out deletion in small batches of data. • A HSE staff member should contact National Service Desk for technical support when preparing to delete a large collection of data (e.g. on disposition when the retention period has expired for a large collection of records).

8.2 Appendix II: National Implementation Plan

The ongoing monitoring, audit and evaluation aims to support the sustained implementation of the updated policy. The Audit Checklist for the Implementation of the HSE National Records Retention Policy in Appendix V intends to assist the initial and sustained implementation at the service delivery area.



8.3 Appendix III: Audit Checklist for the Implementation of the HSE National Records Retention Policy

Purpose: This checklist will help relevant functional areas[1] to audit their compliance with the key guidance and recommendations in the policy.
Responsibility: Managers are required to complete this checklist[2] and incorporate any identified area for improvement into their local implementation plan[3].

Methodology			
Population: A sample of target users Sampling: A total of 10% or 10 target users, whichever is greater, should be selected. Frequency: To be determined locally at least annually. Method: Record **Y** for Yes, if the criteria are met. Record **N** for No, if criteria are not met or **N/A** for Not applicable. Compliance requirement: 100% compliance			
Is standard/criteria being met for the following statements:	**Y/N/Na**	**Possible Remedial Actions / Comments**	**Due Date**
Have you/your team located and read the HSE National Information Classification Handling Policy?			
Are roles and responsibilities communicated to all identified responsible persons? *[Section 3.1 Roles and Responsibilities]*			
Do you know what range of record you use in your area (what types/categories of data, whose data e.g. employees, service users, etc.)? *[Section 1.2 Scope]*			
Do you use data that you collect only for the purposes for which they were originally collected (or have a have a legal basis to do otherwise)? *[Section 3.2 Records Retention and GDPR]*			
For your records not listed in the policy, have you given due consideration to regulatory, operational requirements or input from your engagement with relevant stakeholders to balance what retention period would be appropriate, necessary, and justifiable? *[Section 3.6.1 Deciding on Retention Periods if Records are not listed in the Schedule]*			
When a decision is made to deviate from the policy's retention schedules, have you considered the number of factors set out in the policy? *[Section 3.5 Policy Exceptions]*			

[1] For the purposes of this checklist, 'functional areas' can be defined as your immediate team or work area.
[2] Once completed, you can choose to file it in your local recordkeeping system to provide a benchmark for your own reference purposes.
[3] 'Local Implementation Plan', each service area is responsible for applying HSE National Records Retention Policy 2025 and creating a local implementation plan.

When a decision is made to deviate from the policy's retention schedules, please specify the rationale or the location of the relevant document. *[Section 3.5 Policy Exceptions]*			
Do you maintain records only for as long as necessary? [*Section 3.2 Records Retention and GDPR]* Conduct a sample audit of record types to ensure that: • The required records are within retention periods (select a sample) • Records that are outside of retention periods no longer exist, and have been properly disposed of *By performing this audit with a selection of users annually, each record type should be reviewed at least once over a 5-year cycle (or thereabouts)			
Has a clinical-governance representative (which may include nursing or midwifery representation, as appropriate) reviewed audit findings to ensure that record-management standards and professional-practice obligations are being maintained?			

Date of Audit:	
Audited by (name/title):	
Compliance Rate %:	

Calculation of Compliance Rate %:
The score, expressed as a percentage, is calculated by dividing the number of “yes” and “no” answers. “Not applicable” answers are excluded from the calculation of the percentage score.

Example: If there are 6 “yes” and 2 “no” answers, the score is calculated as follows:
6 (yes answers) divided by 8 (total of yes and no answers) multiplied by 100 = 75%

If a decision is made to deviate from the retention schedules in the policy, that as well as “consider[ing] the number of factors set out in the policy”, that the rationale would be documented too. Just need to be sure that if this is reviewed, that someone knows why “yes” was ticked if the person who conducted the audit has retired or moved or can’t remember the context why deviation was necessary.

8.4 Appendix IV: National Records Management Programme Group Membership

Name	Division
Ann Sheehan	Chairperson, PICRM
Colette Burke	PICRM
Stephen Biesty	Office of the commission of Investigations
Lorraine O'Leary	PICRM
Emma Dardis	DPO
Fiona Moran	Dublin North-East
Angela Maher	DPO
Caroline Crawford	West North-West
Carmel Burke	National Services and Schemes
Martin Quinlivan	Procurement
Fiona Collins	South-West
Kay Kennington	Mid-West
Sadhbh Eavan Brangan	Dublin South-East
Eibhlín Ní Oisín	M365 Information Governance
Eileen Cronin	Southwest
Liam Quirke	West North-West
James Conway	Dublin and Midlands

8.5 Appendix V: Membership of Approval Governance Group

Membership of [name of Approval Governance Group]	
Name	**Role and position**
Joe Ryan	Chairperson, National Director, Public Involvement, Culture & Risk Management
Tom Laffan	Chief Data & Analytics Officer
Stephen Biesty	Office of Commission of Investigations
Mary Deasy	Data Protection Officer
Brian O'Connell	National Director, Health Infrastructure
Noreen Hynes	General Manager, Chief Data and Analytics
Ann Sheehan	General Manager, Public Involvement, Culture & Risk Management
Tony Canavan	REO, West North West
Carmel Burke	Assistant National Director, National Schemes
Loretto Grogan	Chief Nursing & Midwifery information Officer
Gareth Morten	National Director, Procurement
Cliodhna Byrne	Chief Architect

Sign-off by Chair of Approval Governance Group

HSE National Information Classification Handling Policy V2 was formally ratified and recorded in the minutes of the Senior Management Team (SMT) on 20/10/2026.

Name: (print)	Joe Ryan
Title:	National Director, PICRM
Signature: **(e-signatures accepted)**	
Registration number: **(if applicable)**	N/A

**The approval of the document must be an agenda item at the approval governance group meeting for formal ratification. The date of approval must be recorded on the front page of this template*

8.6 Appendix VI: Signature sheet

This is a tool for line managers to print off and have staff sign as part of good record keeping/audit trail.

I have read, understand and agree to adhere to this Policy / Procedure/ Protocol/ Guideline/ Clinical Guideline (delete as appropriate)

Document Title: HSE National Information Classification and Handling Policy

Print Name	Signature	Job Title	Date