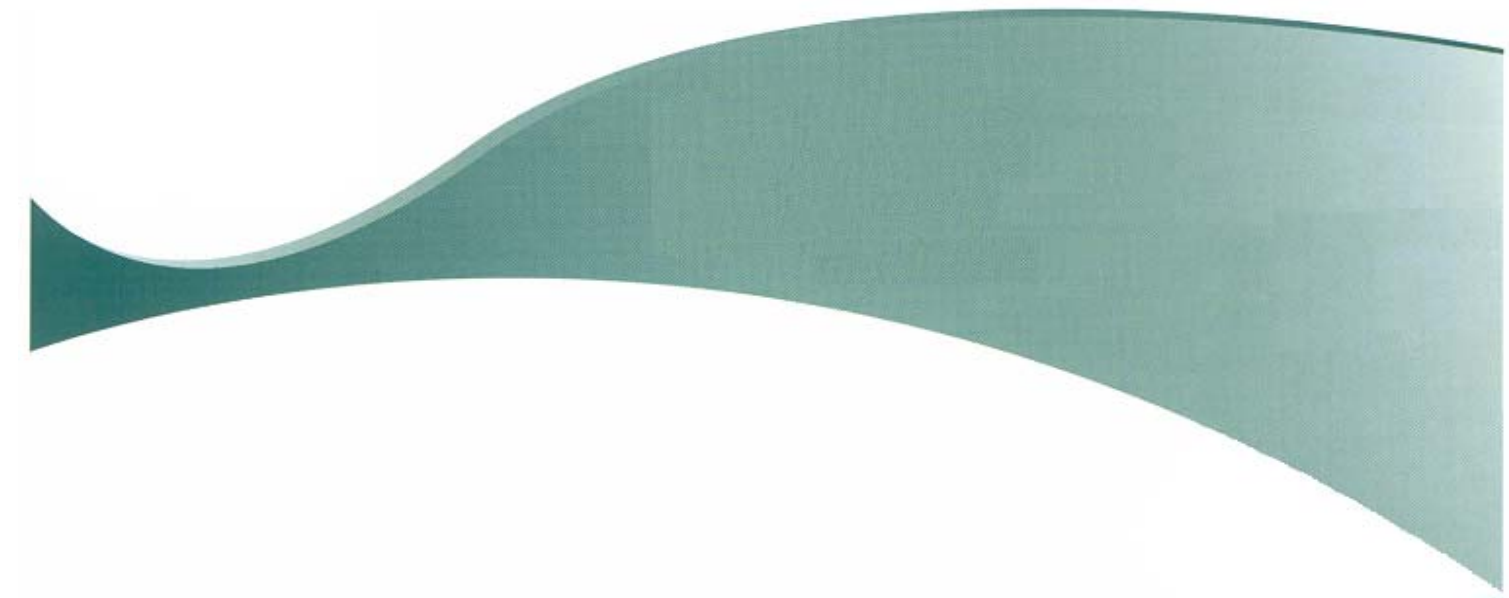
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Information Classification & Handling Policy



Version 1.0

This policy maybe updated at anytime (without notice) to ensure changes to the HSE's organisation structure and/or business practices are properly reflected in the policy. Please ensure you check the HSE intranet for the most up to date version of this policy

http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/

Reader Information

Title:	HSE Information Classification & Handling Policy.
Purpose:	To ensure all the information processed within the HSE is classified and handled appropriately.
Author:	Information Security Project Board (ISPB) on behalf of the HSE.
Publication date:	February 2013
Target Audience:	All HSE staff, students, contractors, sub-contractors, agency staff and authorized commercial service providers that use the organizations IT resources.
Superseded Documents:	All relevant local HSE information classification policies and procedures.
Related Documents:	HSE Information Security Policy. HSE Electronic Communications Policy. HSE Password Standards Policy. HSE Encryption Policy. HSE Mobile Phone Device Policy. HSE Access Control Policy. HSE Service Provider Confidentiality Agreement. Data Protection Acts 1988 & 2003 Freedom of Information Acts 1997 & 2003
Review Date:	February 2014
Contact Details:	Chris Meehan ISPB Secretary, ICT Directorate Dr.Steevens Hospital Steevens Lane Dublin 8 Email: chris.meehan@hse.ie

Document History

Version	Owner	Author	Publish Date
1.0	HSE	Information Security Project Board (ISPB)	February 2013

1.0 Purpose

The Health Service Executive (HSE) creates, collects and processes a vast amount of information in multiple formats everyday. The HSE has a responsibility to protect this information and ensure its confidentiality, integrity and availability.

The HSE is committed to the correct and proper classification and handling of this information. 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 organization. The classification assigned places controls relating to the type of information and its need to remain confidential and secure.

The appropriate classification, handling and storage of information is the responsibility of every 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

2.0 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 all:

- HSE Information;
- Directorates and Service Areas;
- HSE staff and students;
- HSE contractors and sub-contractors;
- Agency personnel working on behalf of the HSE;
- Third party commercial service providers.

3.0 Definitions

A list of terms used throughout this policy are defined in *Appendix A.*

4.0 Policy

4.1 Information Classification

All information (irrespective of its format) owned, created, received, stored and processed by the HSE must be classified according to the sensitivity of its contents. Classification controls should take account of the organizational 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:

1) **Public**

2) **Internal**
3) **Confidential**
4) **Restricted**

The information classification matrix on *page 7* outlines the different categories of HSE information and lists some examples of each.

4.1.1 Public Information

Public information is defined as information that is available to the general public and is intended for distribution 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 or media releases;
- Pamphlets;
- Advertisements;
- Web content;
- Job postings;
- Public Health Information.

4.1.2 Internal Information

Internal information is defined as information that is only intended for internal distribution among HSE staff, students, contractors, sub-contractors, agency staff and authorized third parties (i.e. service providers etc). 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. Some examples of internal information include:

- Internal telephone directory;
- Internal policies & procedures (excluding those published on the web);
- User manuals;
- Training manuals and documentation;
- Staff newsletters & magazines;
- Inter-office memorandums (depending on the content);
- Business continuity plans.

4.1.3 Confidential Information

Confidential information is defined as information which is protected by Irish and/or E.U. legislation or regulations, HSE policies or legal contracts. 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 (Except that which is restricted);
- Patient /client / staff medical records (Except that which is restricted);
- Unpublished medical research;
- Staff personal records;
- Financial information / budgetary reports;
- Service plans / service performance monitoring reports;
- Draft reports;
- Audit reports;
- Purchasing information;
- Vendor contracts / commercially sensitive information;
- Information covered by non-disclosure / confidentiality agreements;
- Passwords / cryptographic private keys;
- Information collected as part of criminal/HR investigations;
- Incident reports.

4.1.4 Restricted Information

Restricted information is defined as highly sensitive 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. Some examples of restricted information include:

- Patient / client / staff sensitive personal information (i.e. 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.

HSE Information Classification Matrix

Topic	Public	Internal	Confidential	Restricted
Definition	Information that is available to the general public and intended for distribution outside the HSE. This information may be freely disseminated without potential harm.	Information that is only intended for internal distribution 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 E.U. legislation or regulations, HSE policies or legal contracts	Highly sensitive confidential information
Examples The examples listed are only provided for guidance purposes and should not be seen as an exhaustive list.	• Patient/Client brochures; • Staff brochures; • News or media releases; • Pamphlets; • Advertisements; • Web content; • Job postings; • Public Health Information.	• Internal telephone directory; • Internal policies & procedures (excluding those published on the web); • 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; • Incident reports; • Information collected as part of criminal/HR investigations.	• Patient / client / staff sensitive personal information (i.e. 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.
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.

4.2 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. The information handling matrix in ***Appendix B*** specifies how the different classifications of information must be handled.

5.0 Roles & Responsibilities

5.1 Information Owners

Information owners are responsible for:

- The full implementation of this policy and all other relevant policies within the HSE directorate or service they manage;
- Ensuring all information (irrespective of its format) owned, created, received, stored and processed within the HSE directorate or service they manage is classified and handled in accordance with this policy;
- Making sure adequate procedures are implemented within their directorate or service, so as to ensure all HSE staff, students, contractors, sub-contractors, agency staff, third parties and others that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies;
- Making sure adequate procedures and training programs are implemented within their directorate or service to ensure on-going compliance of this policy and all other relevant 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 accordance 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 accordance with this policy;

- Reporting all misuse and breaches of this policy to their line manager.

5.4 Contractors, Sub-contractors & 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 accordance with this policy;

- 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 accordance with this policy;

- Reporting all misuse and breaches of this policy to their HSE contact.

6.0 Enforcement

- The HSE reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. HSE staff, students, contractors, sub-contractors or agency staff who breach this policy maybe subject to disciplinary action, including suspension and dismissal as provided for in the HSE disciplinary procedure.

- Breaches of this policy by a third party commercial service providers, may lead to the withdrawal of HSE information technology resources to that third party commercial service provider and/or the cancellation of any contract(s) between the HSE and the third party commercial service provider.

7.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary to ensure any changes to the HSE's organisation structure and business practices are properly reflected in the policy.

The most up to date version of this policy is published on the HSE intranet (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/*

Appendix A

Anonymised / Anonymisation: The process of rendering information into an irrevocable form which does not identify any individual and can no longer be linked to an individual.
.

Authorisation / Authorised: Official HSE approval and permission to perform a particular task.

Backup: The process of taking copies of important files and other information stored on a computer to ensure they will be preserved in case of equipment failure, loss or theft etc.

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.

Electronic Media: Any information that has been created and is stored in an electronic format, including but not limited to software, electronic documents, photographs, 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 information communication system that interconnects different HSE Local Area Networks (LAN) and Wide Area Networks (WAN).

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), National Director **(**or equivalent)).

Information System: A computerized system or software application used to access, record, store, gather and process information.

Information Technology (I.T.) resources: Includes all computer facilities and devices, networks and information communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and information that are owned or leased by the HSE.

Line manager: The individual a user reports directly to.

Macerate / Macerated: Destruction by dissolving in chemicals.

Mobile Computer Device: Any handheld computer device including but not limited to laptops, notebooks, tablet computers, iPads, smartphone devices (e.g. PDA, iPhone and Blackberry enabled devices, etc).

Mobile Phone Device: Any wireless telephone device not physically connected to a landline telephone system. Including but not limited to mobile phones, smartphone devices (e.g. PDA, iPhones, Blackberry enabled devices etc), 3G/GPRS mobile information cards. This does not include cordless telephones which are an extension of a telephone physically connected to a landline telephone system.

Personal information: Information relating to a living individual (i.e. HSE employee, client or patient) who is or can be identified either from the information or from the information in conjunction with other information. For example: - an individuals name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.

Personal Use: The use of the HSE's Information Technology (IT) resources for any activity(s) which is not HSE work-related.
Pulverise / Pulverized: Destruction by grinding into very small pieces or power**.**

Privacy: The right of individual or group to exclude themselves or information about themselves from being made public.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

- Obtaining, recording or keeping the information;
- Collecting, organising, storing, altering or adapting the information;
- Retrieving, consulting or using the information;
- Disclosing the information or information by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, erasing or destroying the information.

Removable Storage Device: Any optical or magnetic 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), external/portable hard drives.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the HSE to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, information management services, patient / client care and management services etc.) to the HSE.

Appendix B

Information Handling Matrix

Information Classification & Handling Procedures				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Document Marking	No marking required	No marking required	The front page of all documents to be clearly marked "Confidential" and all subsequent pages to be marked "Confidential" in the header/footer section of the page or stamped appropriately.	The front page of all documents to be clearly marked "Restricted" and all subsequent pages to be marked "Restricted & Confidential" in the header/footer section of the page or stamped appropriately.
Printing, Scanning & Photocopying	No special precautions required.	No special precautions required.	Printing, scanning and photocopying of confidential information **must be kept to a minimum** and only when absolutely necessary. 1) Printers, Scanners and Photocopiers should be located within an area which is not accessible by the general public. 2) Always ensure original documents and copies are removed from printer, scanner or photocopier as soon as possible.	Printing, scanning and photocopying of restricted information **must be kept to a minimum** and only when absolutely necessary. 1) Printers, Scanners and Photocopiers should be located within an area which is not accessible by the general public. 2) Always ensure original documents and copies are removed from printer, scanner or photocopier as soon as possible.
Backup & Recovery	Backed up **weekly** & backup tapes should stored in a safe location when not in use	Backed up **weekly** & backup tapes should stored in a safe location when not in use	Backed up **daily**, preferably onto a secure HSE network server. If backed up locally onto a backup tape instead of a server, then the backup tapes must be stored in a secure location such as a locked filing cabinet, drawer or a safe (preferably a fireproof safe) when not in use. The backup should be tested at least once a month to ensure you can recover the information from the backup tapes in the event of a system crash etc.	Backed up **daily**, preferably onto a secure HSE network server. If backed up locally onto a backup tape instead of a server, the backup tapes must be stored in a secure location such as a locked filing cabinet, drawer or a safe (preferably a fireproof safe) when not in use. The backup should be tested at least once a month to ensure you can recover the information from the backup tapes in the event of a system crash etc.

Information Classification & Handling Procedures				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Access to / disclosure of the information	Available to the general public	Generally made available to all staff, contractors, sub-contractors, agency staff and 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: 1) Accessible to **HSE staff** who have a valid HSE business need to access the information or have been authorised to access the information by the designated HSE information owner. 2) Released and disclosed to the **general public** in accordance with the relevant legislation (*Freedom of Information Act* / *Data Protection Act*) 3) Released and disclosed to **outside organisation's** in accordance with the relevant legislation (*Freedom of Information Act* / *Data Protection Act*) 4) 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 Server Provider Confidentiality Agreement***	Restricted information must only be accessible **On a need to know basis.** Restricted information must only be: 1) Accessible to **HSE staff** who have a valid HSE business need to access the information or have been authorised to access the information by the designated HSE information owner. 2) Released and disclosed to the **general public** in accordance with the relevant legislation (*Freedom of Information Act* / *Data Protection Act*) 3) Released and disclosed to **outside organisation's** in accordance with the relevant (*Freedom of Information Act* / *Data Protection Act*) 4) 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 the ***HSE Server Provider Confidentiality Agreement***

Information Classification & Handling Procedures				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Publication on the Intranet / Internet	Public information which is to be published on the HSE intranet and internet sites must be authorised by the line manager of the HSE section or service area who is responsible for the information.	Internal information which is to be published on the HSE intranet and internet sites must be authorised by the line manager of the HSE section or service area who is responsible for the information.	In accordance with the *HSE Electronic Communications Policy* confidential information **must never** be published, posted or discussed on **any** internet sites, forums, message boards or chat rooms including those sites which are officially sanctioned by the HSE	In accordance with the *HSE Electronic Communications Policy* restricted information **must never** be published, posted or discussed on **any** internet sites, forums, message boards or chat rooms including those sites which are officially sanctioned by the HSE
Breach of Confidentiality • Loss of information • Theft of information • Loss / theft of a computer device containing the information • Actual or suspected unauthorised access • Accidental disclosure	No special requirements	No special requirements	All information breachs involving the actual or suspected loss, theft or disclosure of confidential information must be reported and handled in accordance with the *HSE Data Protection Breach Management Policy*	All information breachs involving the actual or suspected loss, theft or disclosure of restricted information must be reported and handled in accordance with the *HSE Data Protection Breach Management Policy*

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
HSE network server	No special precautions required.	No special precautions required.	1) In accordance with the *HSE I.T. Acceptable Use Policy* confidential information and HSE information systems that store or process such information **should be stored/hosted on a HSE network server** and not stored locally on the hard drive of a laptop or desktop computer. 2) Confidential information stored on a HSE network server which is not stored as part of a HSE information system, must be held within a secure folder which is only accessible by authorised staff.	1) In accordance with the *HSE I.T. Acceptable Use Policy* restricted information and HSE information systems that store or process such information **should be stored/hosted on a HSE network server** and not stored locally on the hard drive of a laptop or desktop computer. 2) Restricted information stored on a HSE network server which is not stored as part of a HSE information system, must be held within a secure folder which is only accessible by authorised staff.
HSE desktop computer	No special precautions required.	No special precautions required.	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, 2) Desktop computer is password protected in accordance with the *HSE Password Standards Policy* and, 3) Desktop computer has been encrypted in accordance with the *HSE Encryption Policy* and, 4) Information is backed up on a regular basis.	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, 2) Desktop computer is password protected in accordance with the *HSE Password Standards Policy* and, 3) Desktop computer has been encrypted in accordance with the *HSE Encryption Policy* and, 4) Information is backed up on a regular basis.

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
HSE laptop computer	No special precautions required.	No special precautions required.	Strictly **prohibited** except where the 1) Storage is necessary for business and/or technical reasons and, 2) Laptop is password protected in accordance with the *HSE Password Standards Policy* and, 3) Laptop computer has been encrypted in accordance with the *HSE Encryption Policy* and, 4) Information is backed up on a regular basis	Strictly **prohibited** except where the 1) Storage is necessary for business and/or technical reasons and, 2) Laptop is password protected in accordance with the *HSE Password Standards Policy* and, 3) The laptop computer has been encrypted in accordance with the *HSE Encryption Policy* and, 4) Information is backed up on a regular basis
HSE mobile computer device • Smart phone device, • Blackberry's • Tablet computer • Notebook computer • PDA • iPhone / iPad	No special precautions required.	No special precautions required.	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, 2) Mobile computer device is password protected in accordance with the *HSE Password Standards Policy* and, 3) Mobile computer device has been encrypted in accordance with the *HSE Encryption Policy* and, 4) Information is backed up on a regular basis	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, 2) Mobile computer device is password protected in accordance with the *HSE Password Standards Policy* and, 3) Mobile computer device has been encrypted in accordance with the *HSE Encryption Policy* and, 4) Information is backed up on a regular basis

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
HSE removable storage devices • CD/DVD • floppy disks/ tapes, • External / portable hard drive • USB Memory Stick	No special precautions required.	No special precautions required.	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, 2) Removable storage device or the confidential information stored on the device has been encrypted in accordance with the *HSE Encryption Policy* and, 3) Information is backed up on a regular basis **Only HSE approved USB memory sticks which are distributed by the ICT Directorate maybe used to store or transfer HSE information**	Strictly **prohibited** except where the 1) Storage is necessary for business or technical reasons and, 2) Removable storage device or the restricted information stored on the device has been encrypted in accordance with the *HSE Encryption Policy* and, 3) Information is backed up on a regular basis **Only HSE approved USB memory sticks which are distributed by the ICT Directorate maybe used to store or transfer HSE information**
HSE photographic or video recording device • Digital cameras • Video cameras • Any devices which are capable of taking still or video recording	No special precautions required.	No special precautions required.	1) In accordance with the *HSE I.T. Acceptable Use Policy* photographic and video recordings taken as part of patient/client treatment and care must be transferred from the photographic or video recording device onto a HSE network server as soon as is practical. When the transfer is complete the photographic / video recording on the device should be deleted. 2) In the event that this can not be carried out immediately the photographic or video recording device should be locked away securely when not in use.	1) In accordance with the *HSE I.T. Acceptable Use Policy* photographic and video recordings taken as part of patient/client treatment and care must be transferred from the photographic or video recording device onto a HSE network server as soon as is practical. When the transfer is complete the photographic / video recording on the device should be deleted. 2) In the event that this can not be carried out immediately the photographic or video recording device should be locked away securely when not in use.

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
HSE audio recording device • Dictaphones • Tape recorders • Any devices which are capable of taking audio recordings	No special precautions required.	No special precautions required.	1) In accordance with the *HSE I.T. Acceptable Use Policy* audio recordings taken as part of patient/client treatment and care must be transferred from the audio recording device onto a HSE network server as soon as is practical. In the event that this can not be carried out immediately the audio recording device should be locked away securely when not in use. 2) When the audio recordings have been transferred to a HSE network server all local copies stored on the audio recording device should be deleted	1) In accordance with the *HSE I.T. Acceptable Use Policy* audio recordings taken as part of patient/client treatment and care must be transferred from the audio recording device onto a HSE network server as soon as is practical. In the event that this can not be carried out immediately the audio recording device should be locked away securely when not in use. 2) When the audio recordings have been transferred to a HSE network server all local copies stored on the audio recording device should be deleted
Staff personal devices (i.e. Where the device is the staff members personal property and is not owned or leased by the HSE)	No special precautions required.	No special precautions required.	**Strictly prohibited in accordance with the** *HSE I.T. Acceptable Use Policy*	**Strictly prohibited in accordance with the** *HSE I.T. Acceptable Use Policy*
Third party off-site storage (i.e. where the storage of the information has been outsourced to a third party company)	No special precautions required.	No special precautions required.	In accordance with the *HSE I.T. Acceptable Use Policy* confidential information may only be hosted and stored off-site by third parties, provided the third party has signed a copy of the ***HSE Server Provider Confidentiality Agreement***	In accordance with the *HSE I.T. Acceptable Use Policy* confidential information may only be hosted and stored off-site by third parties, provided the third party has signed a copy of the the ***HSE Server Provider Confidentiality Agreement***

Storage of Electronic Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Email messages	No special precautions required.	No special precautions required.	Confidential information which is received via email **should not** remain permanently on a local computer once it has been read by the intended recipient. 1) Once the email has been read the confidential information contained within the email message should be moved to a secure folder (with restricted access) on a HSE network server. 2) When the information has been moved to the server all local copies of the email message should be deleted (i.e. delete the copy of the email message in your email inbox and ensure you empty the contents of deleted emails folder). 3) Alternatively the email message and/or the confidential information maybe printed out and stored away in a secure manner (i.e. stored in locked filing cabinets or a secure lockable area with restricted access)	Restricted information which is received via email **should not** remain permanently on a local computer once it has been read by the intended recipient. 1) Once the email has been read the restricted information contained within the email message should be moved to a secure folder (with restricted access) on a HSE network server. 2) When the information has been moved to the server all local copies of the email message should be deleted (i.e. delete the copy of the email message in your email inbox and ensure you empty the contents of deleted emails folder). 3) Alternatively the email message and/or the restricted information maybe printed out and stored away in a secure manner (i.e. stored in locked filing cabinets or a secure lockable area with restricted access)

Storage of Paper & Film Based Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Paper documents and other printed material	No special precautions required.	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: 1) Unauthorised access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. 2) Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc) 3) Deterioration and/or loss	The information must be stored in such a way so as to ensure it is protected against: 1) Unauthorised access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. 2) Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc) 3) Deterioration and/or loss
Microfilm, Microfiche and other image photo negative materials	No special precautions required.	Reasonable precautions to minimise 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: 1) Unauthorised access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. 2) Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc) 3) Deterioration and/or loss	The information must be stored in such a way so as to ensure it is protected against: 1) Unauthorised access. The information should be locked away in a filing cabinet, drawer, safe or records room when it is not in use. 2) Environmental hazards (i.e. fire, flooding, temperature, humidity, atmospheric pollution etc) 3) Deterioration and/or loss

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Spoken word • Conversations • Meetings • Telephone/ mobile calls	No special precautions required	No special precautions required	1) Confidential information should only be discussed with authorised individuals within a private setting. 2) Avoid discussion in public areas such as elevators, hallways, staircases and cafeterias etc. 3) If you have to discuss on the phone ensure you can positively identify the person you are talking to, and preferably use a landline instead of a mobile phone.	1) Restricted information should only be discussed with authorised individuals within a private setting. 2) Avoid discussion in public areas such as elevators, hallways, staircases and cafeterias etc. 3) If you have to discuss on the phone ensure you can positively identify the person you are talking to, and preferably use a landline instead of a mobile phone.

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Internal Post	No special handling required	No special handling required	**Standard internal postal procedure:** 1) If possible, notify recipient in advance. 2) Ensure you have the correct name and address of the intended recipient on the envelope. 3) Send in a sealed inter-office envelope marked "confidential". **Removable storage media:** All CD's, DVD's, diskettes, tapes and other removable storage media containing confidential information must be encrypted in accordance the *HSE Encryption Policy* prior to being sent in the post, and, A process must be in place to ensure the appropriate disposal of the information on removable storage media once the transfer is complete.	**Standard internal postal procedure:** 1) If possible, notify recipient in advance. 2) Ensure you have the correct name and address of the intended recipient on the envelope. 3) Send in a sealed inter-office envelope marked "confidential". **Removable storage media:** All CD's, DVD's, diskettes, tapes and other removable storage media containing confidential information must be encrypted in accordance the *HSE Encryption Policy* prior to being sent in the post, and, A process must be in place to ensure the appropriate disposal of the information on removable storage media once the transfer is complete.

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
External Post	No special handling required	No special handling required	**Standard external postal procedure:** 1) If possible, notify recipient in advance. 2) Ensure you have the correct name and address of the intended recipient on the envelope. 3) Send in a sealed envelope marked "Private & Confidential" and add on a return address where this will not compromise privacy. 4) Send by normal post. **Removable storage media:** All CD's, DVD's, diskettes, tapes and other removable storage media containing confidential information must be encrypted in accordance the *HSE Encryption Policy* prior to being sent in the post, and, A process must be in place to ensure the appropriate disposal of the information on removable storage media once the transfer is complete. **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.	**Standard external postal procedure:** 1) If possible, notify recipient in advance. 2) Ensure you have the correct name and address of the intended recipient on the envelope. 3) Send in a sealed envelope marked "Private & Confidential" and add on a return address where this will not compromise privacy. 4) Send by normal post. **Removable storage media:** In addition to the above, 1) All CD's, DVD's, diskettes, tapes and other removable storage media containing confidential information must be encrypted in accordance the *HSE Encryption Policy* prior to being sent in the post, and, 2) A process must be in place to ensure the appropriate disposal of the information on removable storage media once the transfer is complete. **Bulk postal procedure: same as that for confidential information**

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Internal Email (i.e. to an email address ending in **@hse.ie**)	No special handling required	No special handling required	1) Ensure that the name and email address of the intended recipient are correct. 2) The email message is clearly marked as "Private & Confidential"; 3) Only the minimum amount of confidential information as is necessary for a given function(s) to be carried out is to be sent;	1) Ensure that the name and email address of the intended recipient are correct. 2) The email message is clearly marked as "Private & Confidential"; 3) Only the minimum amount of restricted information as is necessary for a given function(s) to be carried out is to be sent;
External Email (i.e. to an email address **not** ending in @hse.ie)	No special handling required	No special handling required	1) The information transfer must be legally justifiable in accordance with the *Data Protection Act* 2) Ensure that the name and email address of the intended recipient are correct. 3) The email must consist of a title in the subject line to include the word "Confidential" and have an appropriate email disclaimer at the end of the email message. 4) All confidential information included with the email message is encrypted in accordance with the *HSE Encryption Policy* unless the intended recipient email address is hosted on a network which connected to the HSE via a secure connection (for example: VPN, TLS connection etc)	1) The information transfer must be legally justifiable in accordance with the *Data Protection Act* 2) Ensure that the name and email address of the intended recipient are correct. 3) The email must consist of a title in the subject line to include the word "Confidential" and have an appropriate email disclaimer at the end of the email message. 4) All confidential information included with the email message is encrypted in accordance with the *HSE Encryption Policy* unless the intended recipient email address is hosted on a network which connected to the HSE via a secure connection (for example: VPN, TLS connection etc)

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Fax	Use standard HSE fax coversheet and take reasonable care in dialing fax number.	1) Use standard HSE fax coversheet and take reasonable care in dialing fax number. 2) Should not be sent from a fax machine which is located within an area that is accessible to the general public	In accordance with the *HSE Electronic Communications Policy* confidential information should only be sent by fax in exceptional circumstances such as a (1) Medical emergency, (2) Where a legal obligation exists, (3) Informed consent, (4) Where there is no alternative. When confidential information **has** to be sent by fax: 1) The fax machine used to send/receive confidential information should be located within a secure area which is not accessible by the general public. 2) Make sure you are using the correct fax number for the intended recipient. 3) Ensure you use the *HSE Fax Cover Sheet* 4) Where possible, you should telephone the intended recipient before the transmission to ensure they are waiting by the fax machine for the transmission. Subsequent telephone call to confirm receipt of the transmission. 5) Ensure you remove the all documents from the fax machine immediately after faxing.	In accordance with the *HSE Electronic Communications Policy* restricted information should only be sent by fax in exceptional circumstances such as a (1) Medical emergency, (2) Where a legal obligation exists, (3) Informed consent, (4) Where there is no alternative. When restricted information **has** to be sent by fax: 1) The fax machine used to send/receive confidential information should be located within a secure area which is not accessible by the general public. 2) Make sure you are using the correct fax number for the intended recipient. 3) Ensure you use the *HSE Fax Cover Sheet* 4) Where possible, you should telephone the intended recipient before the transmission to ensure they are waiting by the fax machine for the transmission. Subsequent telephone call to confirm receipt of the transmission. 5) Ensure you remove the all documents from the fax machine immediately after faxing.

Transmission of Information				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Electronic File Transfer (EFT)	No special handling required	No special handling required	1) Transmission must be authorised by a HSE line manager (at grade 8 level or above) 2) Information transfer must take place via a secure channel (i.e. Secure FTP, TLS, VPN etc) or the information must be encrypted email in accordance with the HSE Encryption Policy	1) Transmission must be authorised by a HSE line manager (at General Manager level or above) 2) Information transfer must take place via a secure channel (i.e. Secure FTP, TLS, VPN etc) or the information must be encrypted email in accordance with the HSE Encryption Policy
Text Message	No special handling required	No special handling required	Under **no** circumstances whatsoever should confidential information be transmitted by text. However, patients and service users who provide the HSE with prior **explicit consent** maybe reminded by text message of their HSE appointments. Where patients and service users have consented to be contacted by text of their appoints, 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 belonging to patient or service user.**	Under **no** circumstances whatsoever should restricted information be transmitted by text

Physical Security				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Office / Workplace	No special precautions required.	No special precautions required.	1) Access to areas containing confidential information should be restricted to authorised staff only (i.e. manned reception desk, access to office controlled via keypad or swipe card access) 2) Where practical a **clear desk policy** should be in operation where all confidential information (irrespective of format) is cleared from desks and locked away securely when it is not in use.	1) Access to areas containing confidential information should be restricted to authorised staff only (i.e. manned reception desk, access to office controlled via keypad or swipe card access) 2) Where practical a **clear desk policy** should be in operation where all restricted information (irrespective of format) is cleared from desks and locked away securely when it is not in use
Desktop Computers	Desktops computers must be: 1) Password protected in accordance with the ***HSE Password Standards Policy.*** 2) 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	Desktop computers must be: 1) Password protected in accordance with the ***HSE Password Standards Policy.*** 2) 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	Desktop computers must be: 1) Password protected in accordance with the ***HSE Password Standards Policy.*** 2) Password must not be written down on or near the desktop computer 3) 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 4) Positioned in such a way as to minimise the risk of unauthorised individuals accessing the computer or viewing information displayed on the screen.	Desktop computers must be: 1) Password protected in accordance with the ***HSE Password Standards Policy.*** 2) Password must not be written down on or near the desktop computer 3) 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 4) Positioned in such a way as to minimise the risk of unauthorised individuals accessing the computer or viewing information displayed on the screen.

Physical Security				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Laptop Computers	Laptop computers must be: 1) Encrypted in accordance with the ***HSE Encryption Policy*** 2) Password protected in accordance with the ***HSE Password Standards Policy.*** 3) Locked with a laptop cable lock when left in the office overnight or stored in a locked drawer or cabinet 4) Kept with you at all times when working off-site	Laptop computers must be: 1) Encrypted in accordance with the ***HSE Encryption Policy*** 2) Password protected in accordance with the ***HSE Password Standards Policy.*** 3) Locked with a laptop cable lock when left in the office overnight or stored in a locked drawer or cabinet 4) Kept with you at all times when working off-site	Laptop computers must be: ***1)*** Encrypted in accordance with the ***HSE Encryption Policy*** ***2)*** Password protected in accordance with the ***HSE Password Standards Policy.*** 3) Password must not be written down on or near the desktop computer 4) 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 5) Locked with a laptop cable lock when left in the office overnight or stored in a locked drawer or cabinet 6) Kept with you at all times when working off-site	Laptop computers must be: 1) Encrypted in accordance with the ***HSE Encryption Policy*** 2) Password protected in accordance with the ***HSE Password Standards Policy.*** 3) Password must not be written down on or near the desktop computer 4) 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 5) Locked with a laptop cable lock when left in the office overnight or stored in a locked drawer or cabinet 6) Kept with you at all times when working off-site

Physical Security				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Mobile Computer Devices • Smart phones, Blackberry's • Tablet Computer • PDA • iPhone • iPad	Mobile computers devices must be: 1) Encrypted in accordance with the ***HSE Encryption Policy*** 2) Password protected in accordance with the ***HSE Password Standards Policy.*** 3) Kept with you at all times when working off-site 4) Locked away in a filing cabinet or drawer when left in the office overnight	Mobile computers devices must be: 1) Encrypted in accordance with the ***HSE Encryption Policy*** 2) Password protected in accordance with the ***HSE Password Standards Policy.*** 3) Kept with you at all times when working off-site 4) Locked away in a filing cabinet or drawer when left in the office overnight	Mobile computers devices must be: 1) Encrypted in accordance with the ***HSE Encryption Policy*** 2) Password protected in accordance with the ***HSE Password Standards Policy.*** 3) Password must not be written down on or near the desktop computer 4) Kept with you at all times when working off-site 5) Locked away in a filing cabinet or drawer when left in the office overnight	Mobile computers devices must be: 1) Encrypted in accordance with the ***HSE Encryption Policy*** 2) Password protected in accordance with the ***HSE Password Standards Policy.*** 3) Password must not be written down on or near the desktop computer 4) Kept with you at all times when working off-site 5) Locked away in a filing cabinet or drawer when left in the office overnight
Removable Storage Devices • CD/DVD • floppy disks/ tapes, • External hard drive • USB Memory Stick	No special precautions required.	No special precautions required.	1) Encrypted in accordance with the ***HSE Encryption Policy*** 2) Stored in a secure location such as a locked filing cabinet, drawer or a safe (preferably a fireproof safe) when not in use.	1) Encrypted in accordance with the ***HSE Encryption Policy*** 2) Stored in a secure location such as a locked filing cabinet, drawer or a safe (preferably a fireproof safe) when not in use.

Physical Security				
Topic	**Public**	**Internal**	**Confidential**	**Restricted**
Photographic, Video & Audio Recording Devices	Stored in a safe location when not in use	Stored in a safe location when not in use	Stored in a secure location such as a locked filing cabinet, drawer or a safe when not in use.	Stored in a secure location such as a locked filing cabinet, drawer or a when not in use

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of HSE information (irrespective of format) should be made in accordance with the appropriate HSE record retention policies and the *HSE National Hospital Office Code of Practice for Healthcare Records Management – Part 5: Retention and Disposal Schedule*

Topic	Public	Internal	Confidential	Restricted
Paper & Film based information • Paper records & printed material • Microfilm • Micro fiche • Other image photo negative materials	No special requirements, maybe disposed along with general office waste	No special requirements, maybe disposed along with general office waste	Once a senior HSE manager has made the decision to destroy confidential information stored on paper or film material, the material containing the confidential information must be destroyed and disposed of in a secure manner that protects the confidentiality of the information (i.e. shredding (preferably using a cross cut shredder), pulverised, macerated or incineration etc) Where the destruction and disposal of the confidential information is outsourced to a third party service provider, the third party service provider must 1) Sign the the ***HSE Server Provider Confidentiality Agreement*** 2) Provide the subscribing HSE department with a **certificate of information destruction / disposal**	Once a senior HSE manager has made the decision to destroy restricted information stored on paper or film material, the material containing the confidential information must be destroyed and disposed of in a secure manner that protects the confidentiality of the information (i.e. shredding (preferably using a cross cut shredder), pulverised, macerated or incineration etc) Where the destruction and disposal of the restricted information is outsourced to a third party service provider, the third party service provider must 1) Sign the the ***HSE Server Provider Confidentiality Agreement*** 2) Provide the subscribing HSE department with a **certificate of information destruction / disposal**

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of HSE information (irrespective of format) should be made in accordance with the appropriate HSE record retention policies and the *HSE National Hospital Office Code of Practice for Healthcare Records Management – Part 5: Retention and Disposal Schedule*

Topic	Public	Internal	Confidential	Restricted
Computer devices • Laptop Computers • Desktop Computers, • Mobile Computer Devices, • External / Portable Hard Drives, • USB Memory Keys	Must be disposed in accordance with environmental regulations (i.e. WEEE) and have a **certificate of information destruction / disposal**	Must be disposed in accordance with environmental regulations (i.e. WEEE) and have a **certificate of information destruction / disposal**	All traces of confidential information must be removed from old / obsolete laptop/desktop computers, mobile computer devices, removable storage devices (i.e. external hard drives, USB memory sticks) before they are reused within the HSE, sold off to staff, donated to charity, or disposed of. **The deletion or formatting of the confidential information stored on the old/ obsolete device is not sufficient to remove all traces of the information** 1) Where the old / obsolete devices are to be re-used within the HSE, sold off to employees or donated to charity, the information on the devices must be overwritten using special **sanitation software** which is available from the ICT Directorate. 2) Where the old / obsolete devices have come to the end of their working life and are to be disposed off, the devices must be physically destroyed in such a way that it is almost impossible to recover any confidential information stored on the device. This process is usually carried out by a specialist waste disposal company. All computer devices must be disposed in accordance with environmental regulations (i.e. WEEE) and have a **certificate of information destructi**on	Restricted information should be disposed in the same way as confidential information

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of HSE information (irrespective of format) should be made in accordance with the appropriate HSE record retention policies and the *HSE National Hospital Office Code of Practice for Healthcare Records Management – Part 5: Retention and Disposal Schedule*

Topic	Public	Internal	Confidential	Restricted
Photocopiers, Scanners and Fax Machines	Must be disposed in accordance with environmental regulations (i.e. WEEE) and have a **certificate of information destruction / disposal**	Must be disposed in accordance with environmental regulations (i.e. WEEE) and have a **certificate of information destruction / disposal**	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 can not be recovered from the hard drive. This process is usually carried out by a specialist company. All photocopiers, scanners and fax machines devices must be disposed in accordance with environmental regulations (i.e. WEEE) and have a **certificate of information destruction / disposal**	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 restricted information can not be recovered from the hard drive. This process is usually carried out by a specialist company. All photocopiers, scanners and fax machines devices must be disposed in accordance with environmental regulations (i.e. WEEE) and have a **certificate of information destruction / disposal**

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of HSE information (irrespective of format) should be made in accordance with the appropriate HSE record retention policies and the *HSE National Hospital Office Code of Practice for Healthcare Records Management – Part 5: Retention and Disposal Schedule*

Topic	Public	Internal	Confidential	Restricted
CD's & DVD's	No special requirements	No special requirements	The deletion or formatting of old CD/DVD's is not sufficient to remove all traces of confidential information stored on the CD/DVD Old CD/DVD's that contain confidential information must be physically destroyed in such a way that it is almost impossible to recover any of the confidential information stored on the device. For example: • Shredded using a disc shedder • Cut up with a scissors into small pieces • Using sand paper to destroy both surfaces of the CD/DVD • Incineration	The deletion or formatting of old CD/DVD's is not sufficient to remove all traces of restricted information stored on the CD/DVD Old CD/DVD's that contain restricted information must be physically destroyed in such a way that it is almost impossible to recover any of the restricted information stored on the device. For example: • Shredded using a disc shedder • Cut up with a scissors into small pieces • Using sand paper to destroy both surfaces of the CD/DVD • Incineration

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of HSE information (irrespective of format) should be made in accordance with the appropriate HSE record retention policies and the *HSE National Hospital Office Code of Practice for Healthcare Records Management – Part 5: Retention and Disposal Schedule*

Topic	Public	Internal	Confidential	Restricted
Floppy Diskettes, Magnetic Tapes (i.e. backup tapes)	No special requirements	No special requirements	The deletion or formatting of old floppy diskettes and magnetic media is not sufficient to remove all traces of confidential information stored on the floppy diskette or magnetic tape. Old floppy diskettes and magnetic media that contain confidential information must be physically destroyed in such a way that it is almost impossible to recover any confidential information stored on the device. For example: • Degaussing • Pulverised • Incineration	The deletion or formatting of old floppy diskettes and magnetic media is not sufficient to remove all traces of restricted information stored on the floppy diskette or magnetic tape. Old floppy diskettes and magnetic media that contain confidential information must be physically destroyed in such a way that it is almost impossible to recover any confidential information stored on the device. For example: • Degaussing • Pulverised • Incineration

Destruction & Disposal of Information

Note: Any decision to destroy and dispose of HSE information (irrespective of format) should be made in accordance with the appropriate HSE record retention policies and the *HSE National Hospital Office Code of Practice for Healthcare Records Management – Part 5: Retention and Disposal Schedule*

Topic	Public	Internal	Confidential	Restricted
Video & Audio Tapes	No special requirements	No special requirements	The deletion or formatting of old video or audio is not sufficient to remove all traces of confidential information stored on the tape. Old video and audio tapes that contain confidential information must be physically destroyed in such a way that it is almost impossible to recover any confidential information stored on the tape. For example: • Pulverised • Incineration	The deletion or formatting of old video or audio is not sufficient to remove all traces of restricted information stored on the tape. Old video and audio tapes that contain restricted information must be physically destroyed in such a way that it is almost impossible to recover any restricted information stored on the tape. For example: • Pulverised • Incineration