|  |  |
| --- | --- |
| **TITLE** | MedLIS Confidentiality and Acceptable Usage Policy |
| **DOCUMENT NUMBER** | ML-BOP-17 |
| **APPROVED BY** | See Q-Pulse |
| **APPROVAL DATE** | 05.02.2021 |
| **EFFECTIVE DATE** | 25.03.2021 |
| **REVIEW DATE** | See Q-Pulse |
| **AUTHOR (S)** | Susan Kelly |
| **REVIEWED BY** | Miriam Griffin, Joanne Davis, Dara Maher |

**Document Revision History:**

|  |  |  |
| --- | --- | --- |
| **Version No.** | **Date** | **Summary of Changes** |
| **1.0** | 2018 | **Managed off-line** |
| **2.0** | **Dec 2020** | **Version 2: Reformat** |
| **3.0** | **March 2021** | **Section 3 Definitions:**  Include digital signature, CFR11, electronic signature and  electronic record |
| **4.0** |  |  |

**Table of Contents:**

[1.0 Purpose 5](#_Toc67587453)

[1.2 Purpose 5](#_Toc67587454)

[1.3 Scope 5](#_Toc67587455)

[2 SECURITY 6](#_Toc67587456)

[3 Definitions 6](#_Toc67587457)

[3.1 Acronym 10](#_Toc67587458)

[4 Responsibilities 10](#_Toc67587459)

[4.2 ICT Directorate 10](#_Toc67587460)

[4.3 The management and security of the HSE network(LAN/WAN) 10](#_Toc67587461)

[4.4 MedLIS Data controllers (Information Owners) 11](#_Toc67587462)

[4.5 Line Managers 11](#_Toc67587463)

[4.6 Users 12](#_Toc67587464)

[4.7 Network Administrators 13](#_Toc67587465)

[4.8 System Administrators 13](#_Toc67587466)

[5 Equipment/ Materials 13](#_Toc67587467)

[6 Related Documents 13](#_Toc67587468)

[7 Policy 14](#_Toc67587469)

[7.1 Principles of Acceptable Use 14](#_Toc67587470)

[7.2 Monitoring 15](#_Toc67587471)

[7.3 Personal Use 16](#_Toc67587472)

[7.4 Confidentiality and Privacy 16](#_Toc67587473)

[7.5 User Access Accounts & Passwords 18](#_Toc67587474)

[7.6 Software and Electronic Media 19](#_Toc67587475)

[7.7 MedLIS Devices & Equipment 19](#_Toc67587476)

[7.8 Laptops, Mobile Computer Devices & Smart Devices 20](#_Toc67587477)

[7.9 HSE Network 21](#_Toc67587478)

[7.10 Email 23](#_Toc67587479)

[7.11 Information Backup 23](#_Toc67587480)

[7.12 Virus & Malicious Software Protection 23](#_Toc67587481)

[7.13 Information Storage 23](#_Toc67587482)

[7.13.1 MedLIS Server Storage 24](#_Toc67587483)

[7.13.2 MedLIS On-Site Local Storage 24](#_Toc67587484)

[9.17.3 Irish Government Storage Facilities & Data Centres 25](#_Toc67587485)

[7.13.4 Third Party Storage Facilities 25](#_Toc67587486)

[7.13.5 Storage on Personal I.T. Devices & Equipment 26](#_Toc67587487)

[7.14 Physical Security 27](#_Toc67587488)

[7.14.1 Dedicated MedLIS Servers & data communications Equipment 27](#_Toc67587489)

[7.14.2 MedLIS Computers & Peripheral Devices 27](#_Toc67587490)

[7.15 Information Transfer 28](#_Toc67587491)

[7.16 Information Disposal 29](#_Toc67587492)

[7.17 Working from Home (Home Working) 29](#_Toc67587493)

[7.18 Users leaving the MedLIS organisation & User Transfers 31](#_Toc67587494)

[7.19 Information Security Breach 31](#_Toc67587495)

[7.20 Unacceptable Use 32](#_Toc67587496)

[8 Enforcement 33](#_Toc67587497)



# 1.0 Purpose

MedLIS is committed to the correct and proper use of its National Laboratory Information and Electronic Ordering solutions in support of its managerial and service functions.

The inappropriate use of MedLIS (software and hardware) could expose MedLIS to risks including virus and malicious software attacks, theft and unauthorised disclosure of information, disruption of network systems and services or litigation. The purpose of this policy is to provide all MedLIS users including HSE staff, students, GPs, contractors, sub-contractors, agency staff and authorised third party commercial service providers with clear guidance on the appropriate, safe and legal way in which they can make use of the MedLIS applications.

This policy is mandatory and by accessing any MedLIS applications which are owned or leased by the HSE, users are agreeing to abide by the terms of this policy.

## 1.2 Purpose

To provide clear guidance on the appropriate, safe andlegal way in which to use MedLIS, the National Laboratory Information Management System and the accompanying electronic Order Comms solutions.

## 1.3 Scope

This policy represents MedLIS and 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 MedLIS applications provided by the HSE;
* All users (including HSE staff, students, GPs, private consultants, contractors, sub-contractors, agency staff and authorised third party commercial service providers) of the HSE’s I.T resources;
* All use of the MedLIS applications;
* All connections to (locally or remotely) the MedLIS Domains (LAN/WAN/WiFi);
* All connections made to external networks through the HSE network.

# 2 SECURITY

Refer to MedLIS System Security Policy [ML-BOP-6] & MedLIS Policy for Security Controls and System Access [ML-BOP-9].

# 3 Definitions

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

**Authorisation / Authorised:** Official approval and permission to perform aparticular task.

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

**Breach of Information Security:** The situation where HSE confidential or restrictedinformation has been put at risk of unauthorised disclosure as a result of the loss or theft of the information or, through the accidental or deliberate release of the information.

**CFR11:** the part of Title 21 of the Code of Federal Regulations that establishes the United States Food and Drug Administration regulations on electronic records and electronic signatures. Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records

**Confidential information:** As defined by Irish data protection Law and the GDPR. Information which is protected by Irish and/or E.U. legislation orregulations, MedLIS organisations policies or legal contracts. The unauthorised or accidental disclosure of this information could adversely impact MedLIS, its patients, its staff and its business partners. Some examples of confidential information include:

* Patient / client / staff personal data (Except that which is restricted) Patient /client / staff medical records (Except that which is restricted) Unpublished medical research
* Financial data / budgetary Reports
* Service plans / service performance monitoring reports Draft reports
* Audit reports
* Data covered by Non-Disclosure Agreements
* Passwords / cryptographic private keys
* Data collected as part of criminal/HR investigation/incident reports.

**Defamatory:** False statement or series of statements which affect the reputation of aperson or an organisation.

**Digital signature:** means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

**Electronic record:** means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

**Electronic signature:** means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

**Electronic Media:** Any Information that has been created and is stored in an electronicformat, including but not limited to software, electronic documents, photographs, video and audio recordings.

**Encryption / Encrypt:** The process of converting (encoding) information from areadable 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 data (parameter usually a password) used to encrypt/decryptinformation.

**Generic / Group Access Account:** An access account that is intended for use by anumber of different people and not an individual user and as such is not derived from a single user’s name.

**Home Working:** The situation where staff carry out their contractual obligations(either on an occasional or regular basis) on behalf of their MedLIS organisation while working from their home instead of their organisation’s facility.

**Home Worker(s):** Staff are authorised to work from their home (on an occasionalor regular basis) instead of their organisation’s facility.

**HSE Network**: The data communication system that interconnects different HSE LocalArea Networks (LAN), Wide Area Networks (WAN) and Wi-Fi Wireless Networks.

**Cerner Server:** A computer dedicated to Cerner to provide access to Cerner applications and services.

**Information:** Any data in an electronic format that is capable of being processed or hasalready been processed.

**Information Owner:** The individual responsible for the management of a MedLISdirectorate or service.

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

**Intellectual Property:** Any material which is protected by copyright law and gives thecopyright holder the exclusive right to control reproduction or use of the material. For example - books, movies, sound recordings, music, photographs software etc.

**Line manager**: The individual a user reports directly to.

**Mobile Computer Device:** Any handheld computer device including but not limited tolaptops, tablets, notebooks, PDA’s etc.

**Network Administrators:** These are the individuals responsible for the day to daymanagement of a HSE network domain. Also includes personnel who have been authorised to create and manage user accounts and passwords which access the HSE Network.

**Network Domain:** A set of connected network resources (Servers, Computers, Printers,Applications) that can be accessed and administered as group with a common set of rules

**Personal Information:** Information relating to a living individual (i.e. Staff, orpatient or client) 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 MedLIS devices for anyactivity(s) which is not MedLIS related.

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

**Process / Processed / Processing:** Performing any manual or automated operation or setof 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 data by transmitting, disseminating or otherwise making it available;
* Aligning, combining, blocking, erasing or destroying the information.

**Psuedonymised / Pseudonymisation:** Is a process which involves the replacement of allpersonal identifiers (i.e. an individual’s name address etc) contained within information with artificial identifiers (for example replacing an individual’s name and address with their initials or some other code etc). The purpose of pseudonymisation is to make it difficult for any unauthorised third parties to identify any individual(s) from the information, but to allow the organisation who psuedonymised the information in the first place to trace back the information to its origins.

**Removable Storage Device:** Any optical or magnetic storage device or media, includingbut not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick/pen/keys), external/portable hard drives.

**Restricted Information:** (As defined by the*HSE Information Classification & Handling**Policy*) Highly sensitive confidential information**.**The unauthorised or accidentaldisclosure of this information would seriously and adversely impact MedLIS, its patients, its staff and its business partners. Some examples of restricted information include:

* Patient / client / staff sensitive restricted 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

**Smart Device**: A handheld mobile computer device which is capable of wirelessconnection (via WiFi, 3G, 4G etc), voice and video communication and, internet browsing. (for example: Apple IOS enabled devices (i.e. iPhone & iPad), Google Android enabled devices (i.e. Samsung Galaxy tablet), Windows Mobile enabled devices and, Blackberry RIM enabled devices etc

**Software:** A computer program or procedure that enables a computer to perform aparticular task.

**System Administrators:** The individual(s) charged by the designated system owner withthe day to day management of MedLIS information. Also includes the personnel and third parties who have been authorised to create and manage user accounts and passwords on these applications and systems.

**Third Party Commercial Service Provider:** Any individual or commercial companythat have been contracted by the MedLIS organisation 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, data management services, patient / client care and management services etc.) to the MedLIS organisation.

**Third Party Servers and Equipment:** Any servers or computer equipment used to storeor host MedLIS information and/or information systems which are not owned by MedLIS.

**Third Party Storage Facilities:** Any location or facility used to store MedLIS information,which is not owned or managed by the MedLIS organisation.

**Users:** Any authorised individual who uses MedLIS applications.

## 3.1 Acronym

|  |  |
| --- | --- |
| **Acronym** | **Definition** |
| AMS | Cerner Applied Management Services |
| DPIA | Data Protection Impact Assessment |
| GDPR | General Data Protection regulations |
| HSE | Health Services Executive |
| MedLIS | National Medical Laboratory Information System |

# 4 Responsibilities

4.1 It is the responsibility of MedLIS users to deal with data and sensitive information in a responsible manner and to adhere to policies regarding data protection and GDPR.

## 4.2 ICT Directorate

The ICT Directorate is responsible for:

* The provision of reliable computer systems which deploy appropriate technical safeguards against threats to their availability, operation, stability, and performance;

## 4.3 The management and security of the HSE network(LAN/WAN)

* The provision of facilities for information backups on HSE network file servers and other centralized information stores but excluding backups of the hard disks on individual computers;
* The provision and management of anti virus/spyware software throughout the HSE.
* The provision, deployment and management of encryption facilities throughout the HSE.
* The provision of additional security measures to enable use of computer systems outside the normal working environment when this is appropriate and necessary;
* The procurement of all IT networking equipment, software and services; The installation of all software;
* The installation of all IT equipment, including connection to the HSE network; The provision of training, advice and guidance to computer systems users.

## 4.4 MedLIS Data controllers (Information Owners)

Information owners are responsible for:

* The implementation of this policy and all other relevant policies within the directorate or service they manage;
* The ownership, management, control and security of the information processed by their directorate or service on behalf of MedLIS;
* The ownership, management, control and security of MedLIS information systems used by their directorate or service to process information on behalf of MedLIS;
* Maintaining a list of MedLIS applications which are managed and controlled by their directorate or service.
* Making sure adequate procedures are implemented within their directorate or service, so as to ensure all staff, students, contractors, sub-contractors, agency staff and third party commercial service providers that report to them are made aware of and are instructed to comply with this policy and all other relevant policies;
* Making sure staff that report to them are provided with adequate training so as to ensure on-going compliance of this policy and all other relevant policies;

## 4.5 Line Managers

Line managers are responsible for:

* The implementation of this policy and all other relevant MedLIS/HSE/local policies within the business areas for which they are responsible;
* Ensuring that all their staff, students, contractors, sub-contractors and agency staff who report to them are made aware of and have access to this policy and all other relevant MedLIS/HSE/local policies;
* Ensuring that all staff, students, contractors, sub-contractors and agency staff who report to them are provided with adequate training and are instructed to comply with this policy and all other relevant MedLIS policies;
* Ensuring staff, students, contractors, sub-contractors and agency staff who report to them return all MedLIS computer devices (e.g. laptop, smart devices, printer, mobile phone devices, removable storage devices etc) before they leave the employment of the MedLIS organisation or transfer to another MedLIS organisation or service area.
* Reporting all actual or suspected information security breaches immediately to their line manager, data protection officer and the MedLIS back office;

## 4.6 Users

Each user of MedLIS is responsible for:

* Complying with the terms of this policy and all other relevant MedLIS policies, procedures, regulations and applicable legislation;
* Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks;
* Ensuring they only use user access accounts and passwords which have been assigned to them;
* Ensuring all passwords assigned to them are kept confidential at all times and not shared with others;
* Complying with instructions issued by designated information owners, system administrators, network administrators and/or the MedLIS Information Governance body;
* Reporting all lost, stolen or damaged MedLIS devices to their line manager and the MedLIS back office;
* Reporting all actual or suspected information security breaches immediately to their line manager, the data protection officer and the MedLIS back office.
* Reporting all misuse and breaches of this policy to their line manager;
* Ensuring they return to their line manager, all MedLIS computer devices (e.g. laptop, smart devices, printer, mobile phone devices, removable storage devices etc), information, important email messages and other important items (e.g. swipe cards, keys and I.D. badge etc ) before they leave the employment of the MedLIS organisation or transfer to another MedLIS organisation or service area.
* Ensuring they remove or delete all non-MedLIS personal information (i.e. information which is of a personal nature and belongs to the user and not the MedLIS organisation) from their MedLIS device before they leave the employment of the MedLIS organisation, as it may not be possible to get a copy of this data from the organisation once the user has left.

## 4.7 Network Administrators

Each HSE network administrator is responsible for:

* Complying with the terms of this policy and all other relevant HSE policies, procedures, regulations and applicable legislation.

## 4.8 System Administrators

Each MedLIS system administrator is responsible for:

* Complying with the terms of this policy and all other relevant MedLIS policies, procedures, regulations and applicable legislation

# 5 Equipment/ Materials

MedLIS system software/hardware

# 6 Related Documents

MedLIS System Security Policy [ML-BOP-6]

MedLIS Policy for Security Controls and System Access [ML-BOP-9]

MedLIS Change Management Policy [ML-BOP-11]

MedLIS Training Policy [ML-TP-1]

MedLIS DPIA [ML-QP-0019]

MedLIS Quality Manual [ML-QP-0001]

MedLIS Quality Policy [ML-QI-0015]

Joint Controllers Data Sharing Agreement [ML-SLA-0003]

MedLIS Data Protection Breach Management Policy [ML-BOP-22]

HSE Data Breach Policy [ML-IGEX-1]

HSE Data Protection Policy 2018 [ML-EX-0010]

# 7 Policy

## 7.1 Principles of Acceptable Use

The acceptable use of MedLIS applications are based on the following principles:

* All the MedLIS software applications and any information stored on them remain the property of the MedLIS data controllers.
* Users must ensure that they use MedLIS applications at all times in a manner which is lawful, ethical and efficient.
* Users must respect the rights and property of others, including privacy, confidentiality and intellectual property.
* Users must respect the integrity and security of the MedLIS software applications.

## 7.2 Monitoring

MedLIS reserve the right to routinely monitor, log and record any and all use of its applications for the purpose of:

* 1. Helping to trace and resolve technical faults.
  2. Protecting and maintaining network and system security.
  3. Maintaining system performance and availability.
  4. Ensure the privacy and integrity of information stored on the HSE network.
  5. Investigating actual and suspected security incidents.
  6. Preventing, detecting and minimising inappropriate use.
  7. Protecting the rights and property of the HSE and voluntary organisations, its staff, patients and clients.
  8. Ensuring compliance with HSE policies, current legislation and applicable regulations.

Routine auditing reports will be kept by the MedLIS/ HSE for at least 30 days after which time they may be purged or deleted.

MedLIS reserves the right to routinely monitor an individual user’s use of its applications when a breach of its policies or illegal activity is suspected.

The monitoring of an individual user will only be undertaken at the request of the individual’s line manager (at grade 8 level or above) and the HR Directorate. The monitoring may include, but will not be limited to individual login sessions, details of applications and records accessed, downloaded content and the content of electronic communication within the MedLIS applications.

MedLIS will at all times seek to act in a fair manner and respect the individual user’s right for the privacy of their personal information under the *Data Protection Law* and the GDPR.

Information collected through monitoring will not be used forpurposes other than those for which the monitoring was introduced, unless it is clearly in the users interest to do so or it reveals activity that the data controllers could not be reasonably expected to ignore, for example a user found to have illegally accessed and shared patient data must be reported to the Gardaí.

Individual monitoring reports will only be accessible to the appropriate authorised MedLIS data controllers and will be deleted when they are no longer required.

In the process of dealing with MedLIS support calls HSE & Cerner ICT staff may need to access a user’s computer to resolve the support call. In such circumstances ICT staff must respect the privacy of the individual user and not access information, documents or emails of a personal nature without the users permission or unless they need to in order to resolve the support call. In some cases support services may use remote control software to connect and take control of a user’s computer remotely. In such circumstances the support staff will not use this software to connect to the user’s computer without first attempting to contact the user of the computer first.

## 7.3 Personal Use

MedLIS applications are to be used for business-related purposes only. It is illegal to use MedLIS for any personal use.

## 7.4 Confidentiality and Privacy

MedLIS is legally required under the *Irish Data* *Protection Acts* and GDPRto ensure the security and confidentiality of allpersonal information it processes on behalf of its staff, clients and patients.

In accordance with the ***HSE information Classification and handling policy*** ([*http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/ICT/Polici*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_information_Classification_Handling_Policy.pdf) [*es\_and\_Procedures/Policies/HSE\_information\_Classification\_Handling\_Policy.p*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_information_Classification_Handling_Policy.pdf)[*df*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_information_Classification_Handling_Policy.pdf)*)* all MedLIS information (irrespective of its format) must be classified, controlledand handled according to the sensitivity of its contents. Classification controls should take account of the organisational needs for sharing or restricting data and the associated impacts and risks (e.g. consequences if information is mishandled).

In the course of a users’ work he/she may have access to, or hear information concerning the medical or personal affairs of staff members, patients or clients. Such information irrespective of the format (i.e. paper, electronic or otherwise) is strictly confidential and must always be safeguarded.

Users must respect the privacy and confidentiality of information at all times. They must not access information or information systems unless they have a valid business related reason to do so or they have been granted permission by the information owner.

Users must not remove any MedLIS confidential or restricted information (irrespective of format) from the facility they are employed at without the authorisation of their line manager. Such authorisation must be issued in advance of the first instance and may apply thereafter if necessary. Where a user has been authorised to remove MedLIS confidential or restricted information from their facility they will be responsible for the safe transport and storage of the information.

Confidential and restricted information must only be discussed or shared with others on a strict “need to know” basis.

Confidential and restricted information must only be discussed or shared with colleagues or staff of a MedLIS organisation who have a valid business related reason and are authorised to have access to the information.

Confidential and restricted information must only be released and disclosed to the general public in accordance with the relevant legislation and agreed MedLIS and HSE procedures (for example, *Freedom of Information Acts 1997 & 2003* / *Data* *Protection Acts 1988 and 2003 and the GDPR*).

Confidential and restricted information must only be released and disclosed to other governmental agencies and departments in accordance with the relevant legislation (for example, *Freedom of Information Acts 1997 & 2003* / *Data* *Protection Acts / Health (Provision of Information) Act 1997 / Health Acts 1947 to 2007 etc*)

Confidential and restricted information must only be released and disclosed to third party commercial service providers who have:

* 1. A signed contract in place with the MedLIS organisation for the

provision of goods or services to the MedLIS organisation, and;

* 1. A valid legal and business reason for needing access to such

information (for example: they require access to the information in

order to provide the goods or services to the MedLIS organisation), and;

* 1. Signed a copy of the *HSE Service Providers Confidentiality Agreement*

([*http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/I*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/I)[*CT/Policies\_and\_Procedures/Policies/HSE\_Service\_Provider\_Confiden*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf)[*tiality\_Agreement.pdf*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf)).

Where it is necessary to release or disclose confidential or restricted information to third party commercial service providers only the minimum amount of information should be released as is absolutely necessary for a given function to be carried out by the commercial service provider on behalf of the MedLIS organisation.

Confidential or restricted information (irrespective of the format) must not be copied, renamed, deleted or modified without the authorisation of the information owner. This includes information on storage devices and information in transit.

Users must not remove from their MedLIS organisation employment location any confidential or restricted information, (irrespective of the format - paper, electronic or otherwise) belonging to the organisation without the prior authorisation of their line manager.

Personal information which is shared with others for purposes other than medical care, such as medical research or service planning must be first anonymised or psuedonymised otherwise the explicit consent of the patient or client is required.

Personal information belonging to MedLIS organisation staff, patients or clients must not be used for presentations, training or testing purposes unless it has first been anonymised or psuedonymised otherwise the explicit consent of the MedLIS organisation staff, patients or clients is required.

## 7.5 User Access Accounts & Passwords

Refer to MedLIS System Security Policy [ML-BOP-6] and MedLIS Policy for Security Controls and System Access [ML-BOP-9].

Where appropriate, individual users will be granted access to MedLIS applications which are necessary for them to perform their specific function for their MedLIS organisation.

Each authorised user will be assigned an individual user access account name and password set which they can use to access a particular MedLIS applications.

Each user is responsible for all activities performed on any MedLIS application while logged in under their individual access account and password regardless if these activities were performed by the user or not.

Users must ensure all passwords assigned to them are kept secure in accordance with section 4.4 of the *HSE Password Standards Policy* and/or local organisational password standard policies.

Users who suspect their password is known by others must change their password immediately and report any unauthorised use of their credentials.

Users must ensure all default passwords which are supplied by MedLIS or their organisation are changed at initial login to the application.

All access to MedLIS must be controlled and managed in accordance with the *HSE Access Control Policy* and/or local organisational policies. **(**[*http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/ICT/Polici*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Access_Control_Policy.pdf)[*es\_and\_Procedures/Policies/HSE\_Access\_Control\_Policy.pdf*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Access_Control_Policy.pdf)*).*

All passwords used to access MedLIS must be created and managed in accordance with the MedLIS System Security Policy [ML-BOP-6] and MedLIS Policy for Security Controls and System Access [ML-BOP-9]and *HSE Password Standards Policy* and/or local organisational policies. ([*http://hsenet.hse.ie/Intranet/HSE\_Central/Commercial\_and\_Support\_Services/I*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf) [*CT/Policies\_and\_Procedures/Policies/HSE\_Password\_Standards\_Policy.pdf*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf)).

## 7.6 Software and Electronic Media

Each user is responsible for making use of software and electronic media in accordance with the Irish *Copyright and Related Rights Act 2000* and software licensing agreements.

All MedLIS applications developed and purchased on behalf the HSE remains the property of the HSE and must not be used, copied, distributed or borrowed without the authorisation of the HSE.

The ICT Directorate on behalf of the HSE reserves the right to remove software at any time, for reasons including but not limited to non-compliance with MedLIS and HSE policies.

## 7.7 MedLIS Devices & Equipment

All MedLIS devices and equipment provided by the MedLIS project remain the property of the HSE. Users must not remove or borrow MedLIS devices or equipment without the authorisation of their line manager. The security of any MedLIS device and equipment borrowed is the responsibility of the borrower and the MedLIS device and equipment must be returned by the borrower before they leave the employment of the MedLIS organisation or, at the request of the borrower’s line manager or the ICT Directorate.

Users must not alter the hardware or software configuration of any MedLIS device or equipment without the prior authorisation of the MedLIS back office.

Users must take due care when using MedLIS devices and equipment and take reasonable steps to ensure that no damage is caused to the MedLIS device or equipment. They must not use MedLIS devices and equipment (either in a MedLIS facility, while traveling or at home) if they have reason to believe it is dangerous to themselves or others.

Users must report all damaged, lost or stolen MedLIS devices and equipment to their line manager and the MedLIS back office.

Old and obsolete MedLIS devices and equipment must be recycled in accordance with the requirements of the European *Waste Electrical and Electronic Equipment* *(WEEE)* Directive. Users must notify the MedLIS back office of any old I.T. devicesand equipment and they will facilitate the collection and disposal of the devices and equipment.

The MedLIS back office on behalf of the HSE reserves the right to remove any I.T. devices and equipment from the network at anytime, for reasons including but not limited to (1) non-compliance with HSE/ MedLIS organisational policies, (2) the MedLIS device or equipment does not meet approved specification and standard, or (3) the MedLIS device or equipment is deemed to be interfering with the operation of the network.

## 7.8 Laptops, Mobile Computer Devices & Smart Devices

Users must ensure that MedLIS laptops, mobile computer devices and smart devices provided to them are protected at all times*.* They must take all reasonable steps to ensure that no damage is caused to the device and the device is protected against loss or theft.

MedLIS smart devices must only be issued to users who have signed a copy of the *HSE Smart Device User Agreement* ([*http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/ICT/Polici*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/HSE_Smart_Device_Usage_Agreement.pdf) [*es\_and\_Procedures/Forms/HSE\_Smart\_Device\_Usage\_Agreement.pdf*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/HSE_Smart_Device_Usage_Agreement.pdf))

All MedLIS smart devices must be registered with the ICT Directorate/MedLIS back office so that they can be routed through the HSE network infrastructure and managed securely.

MedLIS Laptops, mobile computer devices and smart devices must be password protected in accordance with the *HSE Password Standards Policy* and/or local organisational policy. *(*[*http://hsenet.hse.ie/Intranet/HSE\_Central/Commercial\_and\_Support\_Services/I*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf)[*CT/Policies\_and\_Procedures/Policies/HSE\_Password\_Standards\_Policy.pdf*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf)*).*

Passwords used to access MedLIS laptops, mobile computer devices and smart devices must not be written down on the device or stored with or near the device.

In accordance with the *HSE Encryption Policy* all MedLIS laptops, mobile computer devices and smart devices must have HSE approved encryption software installed or device encryption enabled prior to their use.

*(*[*http://hsenet.hse.ie/Intranet/HSE\_Central/Commercial\_and\_Support\_Services/I*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Encryption_Policy.pdf)[*CT/Policies\_and\_Procedures/Policies/HSE\_Encryption\_Policy.pdf*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Encryption_Policy.pdf)*)*

Confidential and restricted information must only be stored on a MedLIS laptop, mobile computer device or smart device with the authorisation of the user’s line manager (at grade 8 level or above). Such authorisation must be issued in advance of the information being stored on the device. Where authorisation has been granted only the minimum amount of confidential or restricted information must be stored on the device as is absolutely necessary for a given function to be carried out.

When working in the office MedLIS laptops, mobile computer devices and smart devices must be physically secured and positioned in such a way as to minimise the risk of theft. When they have to be left unattended for any period of time and at the end of the each working day the devices should be secured to a desk or some other stationary object using an appropriate locking mechanism (i.e. Laptop / iPad cable lock) or locked in a drawer or filing cabinet.

MedLIS laptops, mobile computer devices and smart devices must not be left unattended when working off-site.

When traveling by car, MedLIS laptops, mobile computer devices and smart devices should be stored securely out of sight when not in use. Avoid leaving the devices unattended in the boot of a car overnight.

When traveling by taxi, train or plane MedLIS laptops, mobile computer devices and smart device’s should be kept close to hand at all times. Avoid placing the devices in locations where they could easily be forgotten or left behind (i.e. in overhead racks or boots of taxis).

When using a MedLIS laptop, mobile computer devices or smart device in a public place users need to take precautions to ensure the information on the device screen cannot be viewed by others.

Users should check before using their MedLIS smart device so as to ensure there is no interference with sensitive electronic medical equipment.

Users must ensure that all MedLIS laptops, mobile computer devices and smart devices provided to them are not accessed (including internet access) by persons who are not MedLIS users (i.e. friends, family members and others etc)

Remote access connections to the HSE network from a MedLIS laptop, mobile computer devices or smart device must be made in accordance with the *HSE* *Remote Access Policy* ([*http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/ICT/Polici*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Remote_Access_Policy.pdf) [*es\_and\_Procedures/Policies/HSE\_Remote\_Access\_Policy.pdf*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Remote_Access_Policy.pdf)).

## 7.9 HSE Network

Refer to MedLIS System Security Policy [ML-BOP-6] and MedLIS Policy for Security Controls and System Access [ML-BOP-9]. Access to HSE network domains and network resources is controlled and managed in accordance with the *HSE Access Control Policy* *(*[*http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/ICT/Polici*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Access_Control_Policy.pdf)[*es\_and\_Procedures/Policies/HSE\_Access\_Control\_Policy.pdf*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Access_Control_Policy.pdf)*)*

Access rights and privileges to the MedLIS domains and HSE network resources will be allocated based on the specific requirement of a users role / function, rather than on their status

Access to HSE network domains will generally be controlled by the use of individual user access account’s.

Remote access connections to MedLIS domains and HSE network resources will be granted and approved in accordance the *HSE Remote Access Policy* *(*[*http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/ICT/Polici*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_remote_Access_Policy.pdf)[*es\_and\_Procedures/Policies/HSE\_remote\_Access\_Policy.pdf*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_remote_Access_Policy.pdf)*).*

Where there is a business need and with the approval of a MedLIS data controller/ information owner or his/her nominee, third party commercial service providers may request and be granted local access (on-site) and/or remote access to MedLIS domains and information systems. Such access request should be managed in accordance with the *HSE Access Control Policy* *(*[*http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/ICT/Polici*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Access_Control_Policy.pdf)[*es\_and\_Procedures/Policies/HSE\_Access\_Control\_Policy.pd****f***](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Access_Control_Policy.pdf)*).*

Third party commercial service providers who are granted local access (on-site) and/or remote access to MedLIS domains and information systems must sign a copy of the *HSE Third Party Network Access Agreement* *(http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/ICT/Polici es\_and\_Procedures/Policies/HSE\_Third\_Party\_Network\_Access\_Agreement.pdf)*

Users must not:

* 1. Disconnect any MedLIS devices, equipment or removable storage devices to or from a HSE network domain without the prior authorisation of the ICT Directorate/ MedLIS back office.
  2. Connect any MedLIS devices and equipment, laptop or smart device to an external network without the prior authorisation of the ICT Directorate.
  3. Connect any I.T. devices and equipment, laptop, smart device, mobile phone device or removable storage device which is their personal property and is not owned or leased by the HSE to a HSE network domain without the prior authorisation of the ICT Directorate

All activity on HSE network domains is routinely monitored, logged and recorded for the purposes of helping to trace and resolve technical faults and investigating actual and suspected security breaches (See section 4.2).

## 7.10 Email

All email use within MedLIS applications is governed by requirements of the *HSE Electronic* *Communications Policy* and/or local organisational Policy*.* (*http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/ICT/Polici*)*.*

## 7.11 Information Backup

Refer to MedLIS System Description [ML-QP-0015].

## 7.12 Virus & Malicious Software Protection

Refer to MedLIS System Security Policy [ML-BOP-6] and MedLIS Policy for Security Controls and System Access [ML-BOP-9].To protect MedLIS applications from computer viruses and other malicious software, no electronic document or file from any source outside of the MedLIS organisation should be opened unless it has first been scanned for known viruses and malicious software. This requirement covers electronic files in any format, including floppy disks, CD’s, DVD’s and email attachments.

The ICT Directorate will ensure virus scanning software is available on every HSE desktop and laptop computer device that is connected to the HSE network and undertake the regular updating of such virus scanning software. Non HSE devices, desktop computers and laptops which are not regularly connected to the HSE network are unlikely to have fully up to date virus protection. Users of these devices are responsible their virus scanning software to be up to date in order to protect the MedLIS applications.

The ICT Directorate is not responsible for supplying or updating virus scanning software on computer devices which are not owned or leased by the HSE.

MedLIS users who receive a virus warning message should send it onto the MedLIS back office to determine the authenticity of the warning. Under no circumstances should they forward it on to other users.

## 7.13 Information Storage

## 7.13.1 MedLIS Server Storage

Refer to MedLIS System Security Policy [ML-BOP-6] and MedLIS System Description [ML-QP-0015]. For security and legal reason the HSE’s preferred position is that:

* 1. All MedLIS confidential or restricted information is stored on dedicated Cerner Servers on the HSE network.
  2. All dedicated Cerner Servers on the HSE Network hosting critical or national information systems, applications, databases, financial systems and management systems should be located within the HSE’s central hosting facility.

Dedicated Cerner Servers are reserved for the hosting/storage of MedLIS/MN-CMS business-related applications and information only. Users must store all non-MedLIS personal information (i.e. information which is of a personal nature and belongs to the user and not the MedLIS organisation) on their local computer device.

## 7.13.2 MedLIS On-Site Local Storage

MedLIS back office may sanction the temporary storage/hosting of a MedLIS application on a MedLIS organisation computer device other than a dedicated Cerner Server network, due to technical or business necessity.

Where a MedLIS application is stored/hosted on a local computer or removable storage device the user of the device and their line manager must ensure the following controls are implemented.

* 1. Where possible the computer or removable storage device is password protected in accordance with the *HSE Password Standards Policy* and/or local organisational policies. ([*http://hsenet.hse.ie/Intranet/HSE\_Central/Commercial\_and\_Support\_Ser*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf) [*vices/ICT/Policies\_and\_Procedures/Policies/HSE\_Password\_Standards\_*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf)[*Policy.pdf*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf))
  2. The confidential and restricted information and/or the computer or removable storage device are encrypted in accordance with the the *HSE* *Encryption Policy and or local organisational policies.* ([*http://hsenet.hse.ie/Intranet/HSE\_Central/Commercial\_and\_Support\_Ser*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Encryption_Policy.pdf) [*vices/ICT/Policies\_and\_Procedures/Policies/HSE\_Encryption\_Policy.pdf*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Encryption_Policy.pdf)
  3. Only the minimum amount of confidential or restricted information’s is as is necessary for a specified task is stored on the computer or removable storage device;
  4. The confidential and restricted information is regularly backed up and the backup copies are stored in a secure place and not with the computer or removable device;
  5. The confidential and restricted information is deleted from computer or removable storage device when it no longer required.

Under no circumstance should unapproved USB memory sticks (encrypted or otherwise) be used to transfer or store MedLIS information.

Removable storage devices and HSE/ Organisation approved encrypted USB memory sticks except those used for backup purposes must not be used for the long-term storage of confidential or personal information.

Photographic, video and audio recordings which are taken as part of a patient’s or client’s treatment and care must be transferred from the recording device (i.e. digital camera, video camera, mobile phone, tape recorder etc) onto a Cerner server as soon as is practical. When the transfer is complete the photographic, video or audio recording on the recording device should be deleted. In the event that this cannot be carried out immediately the recording device should be locked away securely when not in use.

## 9.17.3 Irish Government Storage Facilities & Data Centres

Where Irish government requirements (i.e. shared services) necessitate MedLIS confidential and restricted information and/or information systems maybe physically stored off-site at an Irish Government storage facility or hosted on servers and equipment that are located within an Irish Government data centre.

The storage or hosting of MedLIS information at Irish Government storage facilities or data centres should be covered by appropriate legal contracts and MedLIS must ensure the government department or agency managing the storage or hosting facility has signed a copy of the *HSE Service Provider* *Confidentiality Agreement* ([*http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/ICT/Polici*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf) [*es\_and\_Procedures/Policies/HSE\_Service\_Provider\_Confidentiality\_Agreement.*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf)[*pdf*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf)*).*

## 7.13.4 Third Party Storage Facilities

In special circumstances such as when business, technical (i.e. specialized system support etc), security (i.e. disaster recovery backup etc) or legal (i.e. archiving,) requirements necessitate MedLIS information may be physically stored off-site at a third party storage facility or hosted off-site on third party servers and equipment.

Where MedLIS confidential information, restricted information or information systems are physically stored off-site at a third party storage facility or hosted off-site on third party servers and equipment MedLIS’s preferred position is that third party storage facility, servers and equipment are (1) located within the Republic of Ireland or failing that, (2) they are located within a country which is a member of the European Economic Area (EEA).

In exceptional circumstances MedLIS may consider requests to store / host MedLIS information on third party servers and equipment which are located in a country outside the European Economic Area (EEA). Each request will be evaluated on a case by case basis and will take into account the sensitivity of the information involved, data protection law and any other legal issues, available alternatives, support issues, logistics and the security controls in place.

The storage / hosting of MedLIS off-site at third party storage facilities or on third party servers and equipment must be approved by the relevant information owner.

MedLIS information may only be stored /hosted off-site at third party storage facilities or on third party servers and equipment, when:

* 1. MedLIS has satisfied its self that the third party storing / hosting the MedLIS information has the appropriate human, organisational and technological controls in place to protect the MedLIS information against unauthorised access and disclosure, accidental loss, destruction, deterioration, damage and alteration, and;
  2. A signed legal contract exists between the MedLIS organisation and the third party governing the processing or storage of the MedLIS in and;
  3. The third party has signed a copy of the *HSE Service Provider* *Confidentiality Agreement* ([*http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/IC*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf) [*T/Policies\_and\_Procedures/Policies/HSE\_Service\_Provider\_Confidential*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf)[*ity\_Agreement.pdf*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf)).

## 7.13.5 Storage on Personal I.T. Devices & Equipment

Users are strictly prohibited from hosting/storing MedLIS information on any computer device, mobile computer device, smart device, mobile phone device, removable storage device, photographic, video or audio recording device or any other equipment which is their personal property and is not owned or leased by the HSE and or the MedLIS organisation.

## 7.14 Physical Security

MedLIS devices must be physically secured and positioned in such a way as to minimise the risk of unauthorised individuals accessing the device or viewing information displayed on the device screen.

## 7.14.1 Dedicated MedLIS Servers & data communications Equipment

In circumstances where for technical or business reasons MedLIS servers hosting critical clinical information systems, applications, databases, financial systems or management systems are hosted, the servers should be located within an accessed controlled area (i.e. a server / comms room or a locked room) which are only accessible to authorised HSE staff.

Local file and print servers should be located within an accessed controlled area on-site (i.e. a server / comms room or a locked room) which is only accessible to authorised staff.

Critical HSE network and data communication equipment (for example, switches, routers, hubs, patch panels etc) should be placed in communications racks or cabinets and located within accessed controlled areas (i.e., a server / comms room or a locked room) which are only accessible to authorised staff.

Power and communications cabling carrying data or supporting key information systems should be protected from interception and damage.

Server / comms rooms or other areas housing MedLIS servers and/or network and data communication equipment situated on the ground floor should have all windows kept shut or where possible have shutters installed on the windows.

All staff given access to server / comms rooms or other areas housing HSE network servers and/or network and data communication equipment must be accompanied by an authorised HSE staff member throughout their visit.

Hazardous and combustible materials must not be stored within or near local server / comms rooms or other areas housing HSE network servers and/or network and data communication equipment.

## 7.14.2 MedLIS Computers & Peripheral Devices

Users should operate a clear screen policy and log off or ‘lock’ their computer (using *Ctrl*+*Alt*+*Delete* keys) when they have to leave it unattended for any period of time and at the end of the each working day.

Where practical users should operate a clear desk policy and clear their desks of all confidential and restricted information (irrespective of the format) at the end of each working day or when leaving their workplace for a major part of the day,

Removable storage devices, approved USB memory sticks, laptops, smart devices and photographic, video and audio recording devices should be stored away in a locked cabinet or drawer when not in use.

Where possible, fax machines, printers, scanners and photocopiers which are used to regularly fax, print, scan or copy confidential or restricted information should be located within areas which are not accessible by the general public.

Confidential and restricted information, when faxed, printed, scanned or copied should where practical be collected from the fax machine, printer, scanner or photocopier immediately.

## 7.15 Information Transfer

Transfer(s) of confidential or restricted information to third parties must be authorised by an organisations line manager (at grade 8 level or above). Such authorisation must be issued in advance of the first instance and may apply thereafter if necessary.

Where it is necessary to transfer confidential or restricted information to third parties, only the minimum amount of information should be transferred as is necessary for a given task to be carried out.

Where possible all transfer(s) of confidential and restricted information should take place electronically via secure channels (i.e. Secure FTP, TLS, VPN etc) or encrypted email.

In circumstances where electronic transfer is not possible, confidential or restricted information may be transferred manually using a removable storage device provided the removable storage device or the information is encrypted in accordance with the requirements of the *HSE/ Local Encryption Policy****.*** Where possible the removable storage device should be hand delivered by a staff member to the intended recipient. If this is not possible the removable storage device should be posted to the intended recipient and the intended recipient contacted within a couple of days to confirm they have received the information on the removable storage device. When sending bulk confidential or personal data by post to the same address the use of registered post or some other secure and certifiable delivery method must be used.

All transfer(s) of personal information to third parties must be legally justified and made in accordance with the *Data Protection Acts and GDPR.*

When transferring personal information to a third party located outside the Republic of Ireland there are a number of additional requirements and legal obligations that need to be considered. If any MedLIS organisation has a need to transfer personal information outside the Republic of Ireland they must have approval of their line manager or contact the MedLIS back office.

## 7.16 Information Disposal

Confidential and restricted information must be securely deleted when it is no longer required.

All traces of MedLIS confidential and restricted information must be purged from old MedLIS computers, smart devices, mobile computer devices, mobile phone devices and removable storage devices before they are reused within the MedLIS organisation, sold to staff, donated to charity or recycled.

The simple deletion or formatting of information stored on a device is not sufficient to remove all traces of the information. The information must be purged by either (1) using special sanitation software to overwrite the information a number of times, or (2) the hard disk must be degaussed (i.e. information is permanently purged using a powerful magnet) or (3) the physical destruction of the media (i.e. hard disk, magnetic tape, video & audio tapes, CD/DVD’s, floppy disks etc) the information is stored.

## 7.17 Working from Home (Home Working)

Users who are authorised by their MedLIS organisation to work from home (home workers) must take all reasonable measures to ensure all MedLIS applications provided to them are kept secure and are protected against unauthorised access, damage, loss, theft and computer viruses.

Users who work from home must ensure:

* 1. All work carried out by them on behalf of the MedLIS organisation while working at home is processed and stored on a MedLIS organisation device and not any other device which is their personal property or the personal property of another household member;
  2. All MedLIS devices used by them to work from home are password in accordance with the *HSE Password Standards Policy* and/or local organisational policies ([*http://hsenet.hse.ie/Intranet/HSE\_Central/Commercial\_and\_Support\_Ser*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf) [*vices/ICT/Policies\_and\_Procedures/Policies/HSE\_Password\_Standards\_*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf)[*Policy.pdf*](http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf)).
  3. All devices used by them to work from home have approved encryption software installed;
  4. All devices used by them to work from home have approved anti-virus software installed and this is kept up to date;
  5. All confidential and restricted information which is accessed by them or stored on a MedLIS device provided to them is kept secure and confidential at all times;
  6. All MedLIS devices and information provided to them are not accessed by members of their family, other household members or visitors;
  7. All MedLIS devices and information (irrespective of the format) are securely locked away when not in use;
  8. All remote access connections made from the home workers computer devices to the HSE network are made in accordance with the *HSE Remote* *Access Policy*

***(****http://hsenet.hse.ie/HSE\_Central/Commercial\_and\_Support\_Services/IC*

*T/Policies\_and\_Procedures/Policies/HSE\_Remote\_Access\_Policy.pdf);*

* 1. All old printouts, faxes and other paper based records that contain confidential or restricted information are shredded or disposed of securely and are not disposed along with their ordinary household rubbish;

All devices provided by MedLIS remain the property of MedLIS and must be returned to MedLIS by the home worker before they leave the employment of the MedLIS organisation or at the request of their organisations line manager or the ICT Directorate.

## 7.18 Users leaving the MedLIS organisation & User Transfers

Users must return all MedLIS devices (e.g. laptop, smart devices, printers, 3G cards, removable storage devices, USB memory sticks etc), information (i.e. documents, files etc) and other important items (e.g. swipe cards, keys, parking permit and I.D. badge etc) to their MedLIS line manager before they leave the employment of the MedLIS project.

Line managers must contact the MedLIS back office to ensure that the information system and network access accounts belonging to users leaving the employment of the MedLIS organisation are revoked immediately once they leave the organization.

Users leaving the employment of MedLIS should also ensure they remove or delete all non-MedLIS personal information & email messages (i.e. information / email messages which are of a personal nature and belong to the user and not MedLIS) from their MedLIS device and computer equipment before they leave as it may not be possible to get a copy of this data once they have left the MedLIS organisation.

At the discretion of their line manager users who are retiring or resigning from MedLIS may by agreement purchase their MedLIS computer equipment from the MedLIS back office for their current value. The current value of the computer equipment will be set by the National Director of Finance or his/her nominee.

Line managers must contact the MedLIS back office to ensure that access account privileges that are no longer required by a user as a result of them transferring internally within the MedLIS organisation are removed.

## 7.19 Information Security Breach

Information security breaches include but are not limited to the following

* the loss or theft of a computer device containing confidential or restricted MedLIS information,
* the loss or theft of a photographic, video or audio recording device containing confidential or restricted MedLIS information,
* the loss or theft of a USB memory stick or some other form of removable storage device containing confidential or restricted MedLIS information,
* the transmitting of confidential or restricted MedLIS information by fax or email to an incorrect fax number or email address,
* incidents where confidential or restricted MedLIS information was mistakenly or otherwise disclosed to unauthorised persons.

Users must report all actual or suspected MedLIS information security breaches immediately to their line manager, the Data Protection Officer and the MedLIS back office

Information security breaches must be managed in accordance with the MedLIS/Maternity Information Governance *Data* *Protection Breach Management Policy*

## 7.20 Unacceptable Use

Situations where MedLIS information must not be used:

1. For personal use;
2. For commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
3. For political activities, such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions;
4. To knowingly misrepresent the MedLIS organisation;
5. To transmit confidential or restricted information outside the MedLIS organisation unless the information has been encrypted and transmission has been authorised by their organisational line manager (at grade 8 level or above);
6. To store or transfer confidential or restricted information (encrypted or otherwise) onto an **unapproved** USB memory stick;
7. To enter into contractual agreements inappropriately (i.e. without authorisation or where another form of agreement is required);
8. To create, view, download, host or transmit material (other than users who are authorised by MedLIS to access such material for research etc.) which may generally be considered offensive or and could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs. material is defined as information (irrespective of format), images, video clips, audio recordings etc;
9. To retrieve, create, host or transmit material which is designed to cause annoyance, inconvenience or needless anxiety to others;
10. To retrieve, create, host or transmit material which is defamatory;
11. For any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);
12. For any activity that would compromise the privacy of others;
13. For any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to the MedLIS organisation or others;
14. For any activity that would deliberately cause the corruption or destruction of data belonging to the MedLIS organisation;
15. For any activity that would intentionally waste the MedLIS organisations resources (e.g. staff time and Information Technology (I.T.) resources);
16. For any activity that would intentionally compromise the security of the MedLIS organisations resources, including the confidentiality and integrity of information and availability of support resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection);
17. For the installation and use of software or hardware tools which could be used to probe or break the MedLIS security control
    1. For the installation and use of software or hardware tools which could be used for the unauthorised monitoring of electronic communications within MedLIS
    2. To gain access to information systems or information belonging to MedLIS which you are not authorised to use;
    3. For any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law.

The above list should not be seen as exhaustive, as other examples of unacceptable use of MedLIS resources may exist.

MedLIS refer any use of its information for illegal activities to the Gardai.

# 8 Enforcement

MedLIS reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. Staff, students, contractors, sub-contractors or agency staff who breach this policy may be subject to disciplinary action, including removal of access to the system, 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.

MedLIS will refer any use of its information for illegal activities to the Gardaí.