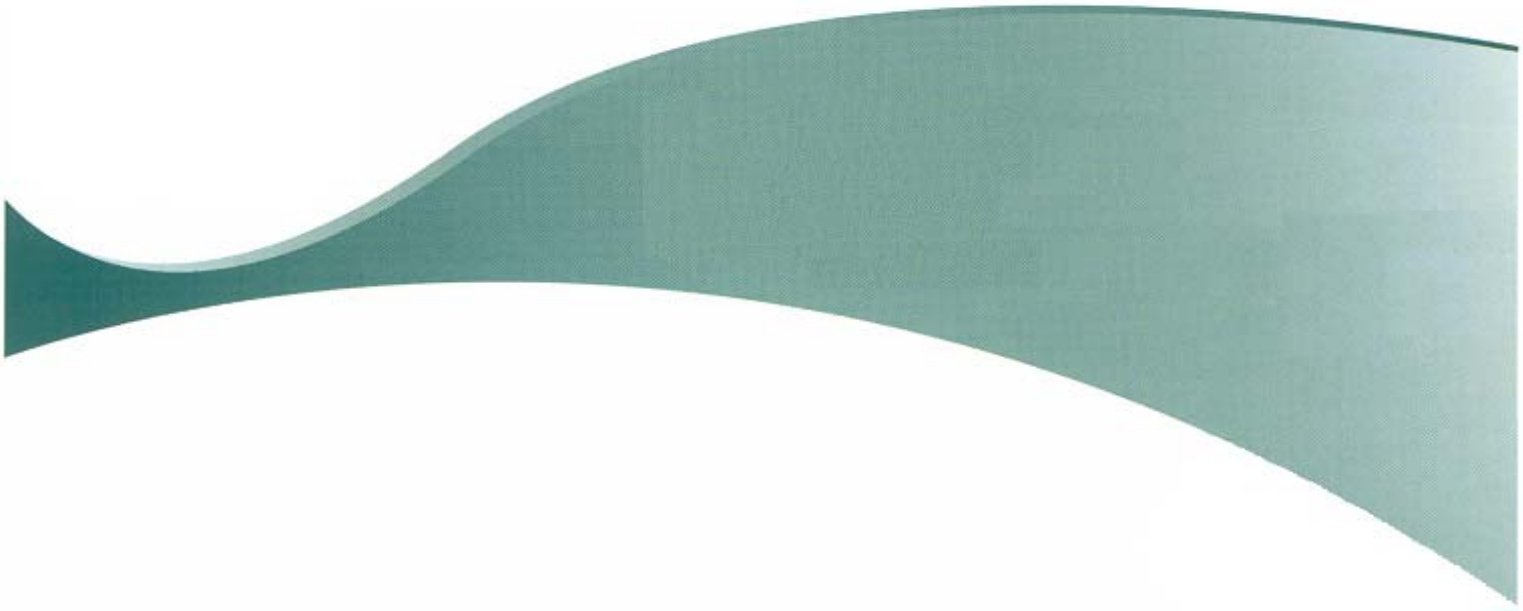
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Information Technology Acceptable Usage Policy



Version 3.0

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 Technology Acceptable Use Policy.
Purpose:	To provide clear guidance on the appropriate, safe and legal way in which to use the HSE's Information Technology resources.
Author:	Information Security Project Board (ISPB) on behalf of the HSE.
Publication date:	February 2013
Target Audience:	All users (including HSE staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the HSE's I.T. resources.
Superseded Documents:	All local Information Technology Acceptable Use Policies and Procedures.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. HSE Information Classification & Handling Policy
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)	June 2009
2.0	HSE	Information Security Project Board (ISPB)	November 2010
3.0	HSE	Information Security Project Board (ISPB)	February 2013

1.0 Purpose

The Health Service Executive (HSE) is committed to the correct and proper use of its Information Technology (I.T.) resources in support of its administrative and service functions.

The inappropriate use of information technology (I.T.) resources could expose the HSE to risks including virus and malicious software attacks, theft and unauthorized disclosure of information, disruption of network systems and services or litigation. The purpose of this policy is to provide HSE staff and other users of its I.T. resources with clear guidance on the appropriate, safe and legal way in which they can make use of the organizations I.T. resources.

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

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 Information Technology (I.T.) resources provided by the HSE;
- All users (including HSE staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the HSE's I.T resources;
- All use (both personal & HSE business related) of the HSE's Information Technology (I.T.) resources;
- All connections to (locally or remotely) the HSE network Domains (LAN/WAN/WiFi);
- All connections made to external networks through the HSE network.

3.0 Definitions

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

4.0 Policy

4.1 Principles of Acceptable Use

The acceptable use of the Health Service Executive's Information Technology (I.T.) resources is based on the following principles:

- All the HSE's I.T. resources and any information stored on them remain the property of the HSE.

- Users must ensure that they use Information Technology (I.T.) resources 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 HSE's Information Technology (I.T.) resources.

4.2 Monitoring

- The HSE reserves the right to routinely monitor, log and record any and all use of its Information Technology (I.T.) resources 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, its staff, patients and clients.
    8) Ensuring compliance with HSE policies, current legislation and applicable regulations.

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

- While the HSE does not routinely monitor an individual user's use of its Information Technology (I.T.) resources it reserves the right to do so 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 information systems and records accessed, contents of hard disks, internet sites visited, time spent on the internet, telephone usage and the content of electronic communications.

- HSE 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 Acts*

1988 & 2003. Information collected through monitoring will not be used for purposes 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 HSE could not be reasonably expected to ignore, for example a user found to be viewing, downloading or forwarding child pornography must be reported to Gardai.

- Individual monitoring reports will only be accessible to the appropriate authorised HSE personnel and will be deleted when they are no longer required.

- In the process of dealing with computer support calls HSE 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 the ICT department may use remote control software to connect and take control of a user's computer remotely. In such circumstances the ICT staff will not use this software to connect to the user's computer without first attempting to contact the user of the computer first.

4.3 Personal Use

- The HSE's Information Technology (I.T.) resources are to be used primarily for HSE business-related purposes. However at the discretion of their line manager occasional personal use may be permitted by a user provided it:

    1) Is not excessive;
    2) Does not take priority over their HSE work responsibilities;
    3) It does not interfere with the performance and work of the user, other staff or the HSE;
    4) Does not incur unwarranted expense or liability for the HSE;
    5) Does not have a negative impact on the HSE in any way;
    6) Does not involve commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
    7) Is lawful and complies with this policy and all other relevant HSE policies

- The HSE has the final decision on deciding what constitutes excessive personal use.

- The HSE does not accept liability for any fraud or theft that results from a user's personal use of the HSE's Information Technology (I.T.) resources.

4.4 Confidentiality and Privacy

- The Health Service Executive (HSE) is legally required under the *Irish Data Protection Acts 1988 & 2003* to ensure the security and confidentiality of all personal 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/Policies_and_Procedures/Policies/HSE_information_Classification_Handling_Policy.pdf*) all HSE information (irrespective of its format) must be classified, controlled and 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 for the HSE, he/she may have access to, or hear information concerning the medical or personal affairs of HSE staff, 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 HSE business related reason to do so or they have been granted permission by the information owner.

- Users must not remove any HSE confidential or restricted information (irrespective of format) from the HSE 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 HSE confidential or restricted information from a HSE 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 other HSE staff or staff of a HSE funded agency who have a valid HSE 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 HSE procedures (for example, *Freedom of Information Acts 1997 & 2003* / *Data Protection Acts 1988 and 2003*).

- 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 1988 and 2003 / 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 HSE for the provision of goods or services to the HSE, and;

    2) 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 HSE), and;

    3) Signed a copy of the *HSE Service Providers Confidentiality Agreement* (*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 HSE.

- 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 HSE employment location any confidential or restricted information, (irrespective of the format - paper, electronic or otherwise) belonging to the HSE without the prior authorization 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 HSE 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 HSE staff, patients or clients is required.

4.5 User Access Accounts & Passwords

- Where appropriate individual users will be granted access to HSE's Information Technology (I.T.) resources which are necessary for them to perform their specific function for the HSE.

- Each authorised user will assigned an individual user access account name and password set which they can use to access a particular HSE Information

Technology (I.T.) resource. In some circumstances the use of generic / group access accounts is permitted (see section 4.3.3 of the *HSE Access Control Policy*).

- Each user is responsible for all activities performed on any HSE I.T. device, information system or application while logged in under their individual access account and password.

- Users must ensure all passwords assigned to them are kept secure in accordance with section 4.4 of the *HSE Password Standards Policy*.

- Users who suspect their password is known by others must change their password immediately.

- Users must ensure all default passwords which are supplied by a vendor for new HSE I.T. devices and information systems are changed at installation time.

- All access to HSE Information Technology (I.T.) resources must be controlled and managed in accordance with the *HSE Access Control Policy* (*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 HSE Information Technology (I.T.) resources must be created and managed in accordance with the *HSE Password Standards Policy* (*http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf*).

4.6 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.

- Only software which has the correct and proper license may be installed and used within the HSE.

- Mobile and smart device application software (i.e. apps) must only be downloaded and installed on HSE smart devices where there is a valid HSE business reason and the software can add value to the users work for the HSE.

- All software and electronic media 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 (1) non-compliance with HSE

policies, (2) the software is not properly licensed, or (3) the software is found to have a negative impact on the performance of the HSE network, systems or equipment.

4.7 HSE I.T. Devices & Equipment

- All HSE I.T. devices and equipment must be purchased through the following agreed channels, national HSE contract agreements, ICT framework agreements or directly through the ICT Directorate.

- HSE I.T. devices and equipment which has not been purchased through agreed channels must be approved by the ICT Directorate before being allowed to connect to the HSE network.

- All I.T. devices and equipment provided by the HSE remain the property of the HSE. Users must not remove or borrow HSE I.T. devices or equipment without the authorisation of their line manager. The security of any HSE I.T. devices and equipment borrowed is the responsibility of the borrower and the I.T. devices and equipment must be returned by the borrower before they leave the employment of the HSE 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 HSE I.T. device or equipment without the prior authorisation of the ICT Directorate.

- Users must take due care when using HSE I.T. devices and equipment and take reasonable steps to ensure that no damage is caused to the I.T. device or equipment. They must not use I.T. devices and equipment (either in a HSE 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 HSE I.T. devices and equipment to their line manager and the ICT Directorate.

- Old and obsolete HSE I.T. 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 ICT Directorate of any old I.T. devices and equipment and they will facilitate the collection and disposal of the devices and equipment.

- The ICT Directorate 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 policies, (2) the I.T. device or equipment does not meet approved specification and standard, or (3) the I.T. device or equipment is deemed to be interfering with the operation of the network.

4.8 Laptops, Mobile Computer Devices & Smart Devices

- Users must ensure that HSE 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.

- HSE 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/Policies_and_Procedures/Forms/HSE_Smart_Device_Usage_Agreement.pdf*)

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

- HSE Laptops, mobile computer devices and smart devices must be password protected in accordance with the *HSE Password Standards Policy* (*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 HSE 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 HSE laptops, mobile computer devices and smart devices must have HSE approved encryption software installed or device encryption enabled prior to their use within the HSE. (*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 HSE laptop, mobile computer device or smart device with the authorization 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 authorization 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 HSE 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.

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

- When traveling by car, HSE 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.

- The use of HSE smart devices within a car must at all times be made in accordance with the *Road Traffic Act 2006.*

- When traveling by taxi, train or plane HSE 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 HSE 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 HSE smart device to make and accept phone calls within HSE premises and other clinical/medical facilities so as to ensure there is no interference with sensitive electronic medical equipment.

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

- Remote access connections to the HSE network from a HSE 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/Policies_and_Procedures/Policies/HSE_Remote_Access_Policy.pdf*).

4.9 HSE Network

- 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/Policies_and_Procedures/Policies/HSE_Access_Control_Policy.pdf)*

- Access rights and privileges to the HSE network domains and network resources will be allocated based on the specific requirement of a users HSE 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, however in certain circumstances the use of generic or group accounts maybe permitted (see section 4.3.3 of the *HSE Access Control Policy*).

- Remote access connections to HSE network domains and 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/Policies_and_Procedures/Policies/HSE_remote_Access_Policy.pdf).*

- Where there is a business need and with the approval of a HSE 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 the HSE network 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/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 the HSE network domains and information systems must be sign a copy of the *HSE Third Party Network Access Agreement (http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Third_Party_Network_Access_Agreement.pdf)*

- Users must not:

    1) Disconnect any HSE I.T. devices, equipment or removable storage devices to or from a HSE network domain without the prior authorisation of the ICT Directorate.

    2) Connect any HSE I.T. 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).

4.10 Email

- All email use within the HSE is governed by requirements of the *HSE Electronic Communications Policy* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Electronic_Communications_Policy.pdf*).

4.11 Internet

- All internet use within the HSE is governed by requirements of the *HSE Electronic Communications Policy* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Electronic_Communications_Policy.pdf*).

4.12 Telephone System

- Access to the HSE telephone system is primarily intended for HSE work related purposes. The making and taking of personal calls is allowable provided users keep these to a minimum.

- Users must respect the privacy of others at all times and not attempt to access calls where the user is not the intended recipient or log into voice mail accounts that the user is not expressly authorised to access.

- The use of HSE mobile phone devices is governed by the requirements of the *HSE Mobile Phone Device Policy* **(***http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Mobile_Phone_Device_Policy.pdf*).

- The use of HSE facsimile (fax) machines is governed by the requirements of the *HSE Electronic Communications Policy* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Electronic_Communications_Policy.pdf*).

4.13 Information Backup

- Where an agreement exists between the ICT Directorate and the information owner, HSE network servers will be automatically backed up on a daily basis.

- Users who do not have access to a HSE network server must ensure that they regularly backup all their important information onto another computer or a removable storage device. Each user is responsible for ensuring their backup information is kept safe and secure.

- Information backups especially those containing confidential and restricted information must be stored securely in a locked drawer, filing cabinet or safe.

- Information backups should be regularly tested to ensure that a recovery can take place following an incident or hardware/software failure.

4.14 Virus & Malicious Software Protection

- To protect the HSE from computer viruses and other malicious software, no electronic document or file from any source outside of the HSE 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. Due to their nature standalone 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 computer devices must contact the ICT Directorate at least once a month and have their virus scanning software updated manually.

- 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.

- Users who receive a virus warning message should send it onto the ICT Directorate to determine the authenticity of the warning. Under no circumstances should they forward it on to other users.

4.15 Information Storage

4.15.1 HSE On-Site Server Storage

- For security and legal reason the HSE's preferred position is that:

    1) All HSE confidential or restricted information is stored on a HSE network server.

    2) All HSE network servers hosting critical or national information systems, applications, databases, financial systems and management systems should be located within the HSE's central hosting facility.

    3) All other HSE network servers which host HSE information systems that process confidential or restricted information are located on-site within HSE managed facilities.

- Confidential or 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 users.

- HSE network servers are reserved for the hosting/storage of HSE business-related systems and information only. Users must store all non-HSE personal information

(i.e. information which is of a personal nature and belongs to the user and not the HSE) on their local HSE computer device.

4.15.2 HSE On-Site Local Storage

- When technical or business requirements necessitate a HSE line manager (at grade 8 level or above) may sanction the temporary storage/hosting of confidential information, restricted information or a HSE information system on a HSE computer device other than a HSE network server.

- Where confidential information, restricted information or a HSE information system 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* (*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* (*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.

- HSE approved encrypted USB memory sticks are available from the ICT Directorate to HSE staff that have a requirement to temporarily store or transfer confidential or restricted information. The USB memory sticks will be issued to HSE staff who have returned a signed copy of the *HSE USB Memory Stick Usage Agreement* to their local ICT department (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/HSE_USB_Memory_Stick_Usage_Agreement.pdf*)

- Under no circumstance should unapproved USB memory sticks (encrypted or otherwise) be used to transfer or store HSE information systems, confidential information or restricted information.

- Removable storage devices and HSE 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 HSE network 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 can not be carried out immediately the recording device should be locked away securely when not in use.

4.15.3 Irish Government Storage Facilities & Data Centres

- Where Irish government requirements (i.e. shared services) necessitate HSE 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 HSE information and systems at Irish Government storage facilities or data centres should be covered by appropriate legal contracts and the HSE 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/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf*).

4.15.4 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 HSE confidential or restricted information and/or information systems maybe physically stored off-site at a third party storage facility or hosted off-site on third party servers and equipment.

- Where HSE 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 the HSE'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 the HSE may consider requests to store / host HSE confidential information, restricted information or information systems 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 HSE confidential and restricted information and information systems off-site at third party storage facilities or on third party servers and equipment must be approved by the relevant information owner.

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

    1) The HSE has satisfied its self that the third party storing / hosting the HSE information and information systems has the appropriate human, organisational and technological controls in place to protect the HSE information and information systems against unauthorized access and disclosure, accidental loss, destruction, deterioration, damage and alteration, and;

    2) A signed legal contract exists between HSE and the third party governing the processing or storage of the HSE information and/or information systems, 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/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf*).

4.15.5 Storage on Personal I.T. Devices & Equipment

- Users are strictly prohibited from hosting/storing HSE confidential information, restricted information or information systems 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.

4.16 Physical Security

- HSE I.T. devices and equipment 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.

4.16.1 HSE Network Servers & data communications Equipment

- In circumstances where for technical or business reasons HSE network servers hosting critical clinical information systems, applications, databases, financial systems or management systems are hosted locally, the 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 HSE staff.
- HSE 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 HSE 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 HSE staff.

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

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

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

4.16.2 HSE Computers & Peripheral Devices

- Users should operate a clear screen policy and log off or ‘lock’ their HSE 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, HSE approved USB memory sticks, mobile phone devices, 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.

4.17 Information Transfer

- Transfer(s) of confidential or restricted information to third parties must be authorised by a HSE 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 maybe 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 Encryption Policy.* Where possible the removable storage device should be hand delivered by a HSE 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 1988 and 2003.*

- 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 HSE Directorate or Service has a need to transfer personal information outside the Republic of Ireland they must contact the ICT Directorate (at infosec@hse.ie) or their local Consumer Affairs department.

4.18 Information Disposal

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

- All traces of confidential and restricted information must be purged from old HSE computers, smart devices, mobile computer devices, mobile phone devices and removable storage devices before they are reused within the HSE, 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 on.

- Photocopiers and scanners which are fitted with hard disks must be purged of all confidential and personal data before they are disposed of or returned to the vendor.

- Computers and other I.T. equipment which are leased from third parties must be purged of all confidential and personal data before being returned to the third party leasing company.

- Where the disposal of old HSE computer equipment and removable storage devices is outsourced to a commercial service provider the commercial service provider must:

    1) Ensure the operation of purging the computer equipment of all confidential and restricted information and the destruction of the media (i.e. hard disk, magnetic tape, video & audio tapes, CD/DVD's, floppy disks etc) is carried out on-site at a HSE facility before the equipment is taken off-site to a licensed WEEE recycling facility within Ireland.

    2) Provide the HSE with a certificate of disposal / destruction for all the equipment that was disposed of / destroyed by them.

3) Signed a copy of the *HSE Service Providers Confidentiality Agreement* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf*).

4.19 Working from Home (Home Working)

- Users who are authorised by the HSE to work from home (home workers) must take all reasonable measures to ensure all the HSE computer devices 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 HSE while working at home is processed and stored on a HSE computer device and not any other device which is their personal property or the personal property of another household member;

2) All HSE computer devices used by them to work from home are password in accordance with the *HSE Password Standards Policy* (*http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf*).

3) All HSE computer devices used by them to work from home have HSE approved encryption software installed;

4) All HSE computer devices used by them to work from home have HSE 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 HSE computer device provided to them is kept secure and confidential at all times;

6) All HSE computer devices and information provided to them are not accessed (including internet access) by members of their family, other household members or visitors;

7) All HSE computer 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/ICT/Policies_and_Procedures/Policies/HSE_Remote_Access_Policy.pdf);

9) 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 computer devices provided by the HSE remain the property of the HSE and must be returned to the HSE by the home worker before they leave the employment of the HSE or at the request of their HSE line manager or the ICT Directorate.

4.20 Periods of Absence

- During planned periods of absence such as career breaks, holidays, on training courses or working off-site for an extended period of time, users should ensure wherever possible that their line manager or work colleagues have access to important HSE business related documents and email messages stored on their computer so that there is no disruption to service delivery.

- During unplanned periods of absence such as ill health, or where a user has forgotten to provide access to their line manager or work colleagues, the user's line manager may be permitted to access their computer to retrieve HSE business related documents or emails messages so as to minimize any disruption to service delivery. In such circumstances line managers must respect the privacy of the user and not access documents or emails of a personal nature unless there are compelling conditions that warrant doing so.

4.21 Users leaving the HSE & User Transfers

- Users must return all HSE mobile phone devices and accessories (e.g. mobile phone car kit and battery charger etc), computer equipment (e.g. laptop, smart devices, printers, 3G cards, removable storage devices, USB memory sticks etc), information (i.e. documents, files, important email messages etc) and other important items (e.g. swipe cards, keys, parking permit and I.D. badge etc) to their HSE line manager before they leave the employment of the HSE.

- Line managers must contact the ICT department to ensure that the information system and network access accounts belonging to users leaving the employment of the HSE are revoked immediately once they leave the organization. (see the *HSE Access Control Policy*)

- Users leaving the employment of the HSE should also ensure they remove or delete all non-HSE personal information & email messages (i.e. information / email messages which are of a personal nature and belong to the user and not the HSE) from their HSE mobile phone 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 HSE.

- At the discretion of their line manager users who are retiring or resigning from the HSE may by agreement purchase their HSE mobile phone device and computer equipment from the HSE for their current value. The current value of the mobile phone device and computer equipment will be set by the National Director of Finance or his/her nominee.

- Users who are transferring internally within the HSE must ensure they return all HSE mobile phone devices and accessories, laptops, and swipe cards etc to their current HSE line manager before they transfer. They must also ensure that their current line manager or work colleagues have access to important HSE business related documents and email messages so that there is no disruption to service delivery after they transfer.

- Line managers must contact the ICT department to ensure that access account privileges that are no longer required by a user as a result of them transferring internally within the HSE are removed. (see the *HSE Access Control Policy*)

4.22 Information Security Breach

- Information security breaches include but are not limited to the following (1) the loss or theft of a computer device containing confidential or restricted information, (2) the loss or theft of a photographic, video or audio recording device containing confidential or restricted information, (3) the loss or theft of a USB memory stick or some other form of removable storage device containing confidential or restricted information, (4) the transmitting of confidential or restricted information by fax or email to an incorrect fax number or email address, (5) incidents where confidential or restricted information was mistakenly or otherwise disclosed to unauthorized persons.

- Users must report all actual or suspected information security breaches immediately to their line manager, the ICT Directorate and/or the Consumer Affairs section.

- Information security breaches must be managed in accordance with the *HSE Data Protection Breach Management Policy* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Data_Protection_Breach_Management_Policy.pdf*).

4.23 Unacceptable Use

- The HSE's Information Technology (I.T.) resources must not be used:

1) For excessive 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 HSE;
5) To transmit confidential or restricted information outside the HSE unless the information has been encrypted and transmission has been authorised by their HSE 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 the HSE to access such material for research etc.) of a pornographic or sexual nature or which may generally be considered offensive or obscene 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 HSE or others;
14) For any activity that would deliberately cause the corruption or destruction of data belonging to the HSE or others;
15) For any activity that would intentionally waste the HSE's resources (e.g. staff time and Information Technology (I.T.) resources);
16) For any activity that would intentionally compromise the security of the HSE's Information Technology (I.T.) resources, including the confidentiality and integrity of information and availability of IT 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 HSE I.T. security controls;

18) For the installation and use of software or hardware tools which could be used for the unauthorised monitoring of electronic communications within the HSE or elsewhere;

19) To gain access to information systems or information belonging to the HSE or others which you are not authorized to use;

20) For creating or transmitting "junk" or "spam" emails. This includes but is not limited to unsolicited commercial emails, jokes, chain-letters or advertisements;

21) 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 the HSE's I.T. resources may exist.
- The HSE has the final decision on deciding what constitutes excessive personal use.
- The HSE will refer any use of its I.T. resources for illegal activities to the Gardai.

5.0 Roles & Responsibilities

5.1 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;
- 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.

5.2 Information Owners

Information owners are responsible for:

- The implementation of this policy and all other relevant policies within the HSE directorate or service they manage;
- The ownership, management, control and security of the information processed by their directorate or service on behalf of the HSE;
- The ownership, management, control and security of HSE information systems used by their directorate or service to process information on behalf of the HSE;
- Maintaining a list of HSE information systems and 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 HSE 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;

5.3 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 that all HSE 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 HSE policies;
- Ensuring that all HSE 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 HSE policies;
- Ensuring staff, students, contractors, sub-contractors and agency staff who report to them return all HSE 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 HSE or transfer to another HSE directorate or service area;

- Reporting all actual or suspected information security breaches immediately to the ICT Directorate and/or the Consumer Affairs section;

- Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

5.4 Users

Each user of the HSE's I.T. resources is responsible for:

- Complying with the terms of this policy and all other relevant HSE 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 ICT Directorate on behalf of the HSE;

- Reporting all lost, stolen or damaged I.T. devices to their line manager and the ICT Directorate;

- Reporting all actual or suspected information security breaches immediately to their line manager, the ICT Directorate and/or the Consumer Affairs section;

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

- Ensuring they return to their line manager, all HSE 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 HSE or transfer to another HSE directorate or service area.

- Ensuring they remove or delete all non-HSE personal information and email messages (i.e. information which is of a personal nature and belongs to the user and not the HSE) from their HSE computer before they leave the employment of the HSE, as it may not be possible to get a copy of this data from the HSE once the user has left the HSE.

5.5 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.

5.6 System Administrators

Each HSE system administrator is responsible for:

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

- Complying with instructions issued by the ICT Directorate on behalf of the HSE.

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.
- The HSE will refer any use of its I.T. resources for illegal activities to the Gardai.

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 data 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 Information Security: 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, through the accidental or deliberate release of the information.

Confidential information: (As defined by the *HSE Information Classification & Handling Policy*) 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 data (Except that which is restricted)
- Patient /client / staff medical records (Except that which is restricted)
- Unpublished medical research
- Staff personal records
- Financial data / budgetary Reports
- Service plans / service performance monitoring reports
- Draft reports
- Audit reports
- Purchasing information
- Vendor contracts / Commercially sensitive data
- Data covered by Non-Disclosure Agreements
- Passwords / cryptographic private keys
- Data collected as part of criminal/HR investigations
- Incident Reports

Defamatory: False statement or series of statements which affect the reputation of a person or an organisation.

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 data (parameter usually a password) used to encrypt/decrypt information.

Generic / Group Access Account: An access account that is intended for use by a number 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 HSE staff carry out their contractual obligations (either on an occasional or regular basis) on behalf of the HSE while working from their home instead of a HSE facility.

Home Worker(s): HSE Staff are authorised to work from their home (on an occasional or regular basis) instead of a HSE facility.

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

HSE Server: A computer on the HSE network used to provide network services and/or manage network resources.

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

Information Owner: The individual responsible for the management of a HSE directorate or service (HSE RDO or 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 I.T. devices and equipment, computer facilities, networks, data & telecommunications systems, equipment and infrastructure, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the HSE.

Intellectual Property: Any material which is protected by copyright law and gives the copyright 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 to laptops, tablets, notebooks, PDA's etc.

Mobile Phone Device: Any wireless telephone device not physically connected to a landline telephone system. Including but not limited to mobile phones, smart phone devices (for example, Apple iPhones, Windows Mobile enabled devices, Google Android enabled devices, Nokia Symbian enabled devices, Blackberry RIM enabled devices etc). This does not include cordless telephones which are an extension of a telephone physically connected to a landline telephone system.

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

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. HSE Staff, or patient 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 the HSE's Information Technology (IT) resources for any activity(s) which is not HSE work-related.

Pornography / Pornographic: The description or depiction of sexual acts or naked people that are designed to be sexually exciting.

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 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 all personal 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 psuedonymisaed 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, 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.

Restricted Information: (As defined by the *HSE Information Classification & Handling Policy*) 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 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 wireless connection (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)

Social Media: The name given to various online technology tools that enable people to communicate easily via the internet to share information and resources. It includes the following types of web sites:

1) **Internet Chat Rooms:** Websites that allow interactive messaging, where users can exchange views and opinions in real time on a variety of subject matters.

2) **Internet Discussion Forums/Message Boards:** Websites that allow users to participate in on-line discussions on a particular subject matter.

3) **Internet Social Networking Websites:** Websites that allow users to build on-line profiles, share information, pictures, blog entries and music clips etc. Including but not limited to Bebo, Facebook, Twitter, Myspace, Friendster, Whispurr, LinkedIn and Viadeo.

4) **Internet Video Hosting/ Sharing Websites:** Websites that allows users to upload video clips, which can then be viewed by other users. Including but not limited to Youtube, Yahoo Video, Google Video and MyVideo.

5) **Blogging Websites:** Websites that allow a user to write an on-line diary (known as a blog) sharing their thoughts and opinions on various subjects

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

System Administrators: The individual(s) charged by the designated system owner with the day to day management of HSE information systems. Also includes the HSE 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 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, data management services, patient / client care and management services etc.) to the HSE.

Third Party Servers and Equipment: Any servers or computer equipment used to store or host HSE information and/or information systems which are not owned by the HSE.

Third Party Storage Facilities: Any location or facility used to store HSE information, information systems and/or computer equipment which is not owned or managed by the HSE.

Users: Any authorized individual who uses the HSE's I.T. resources.