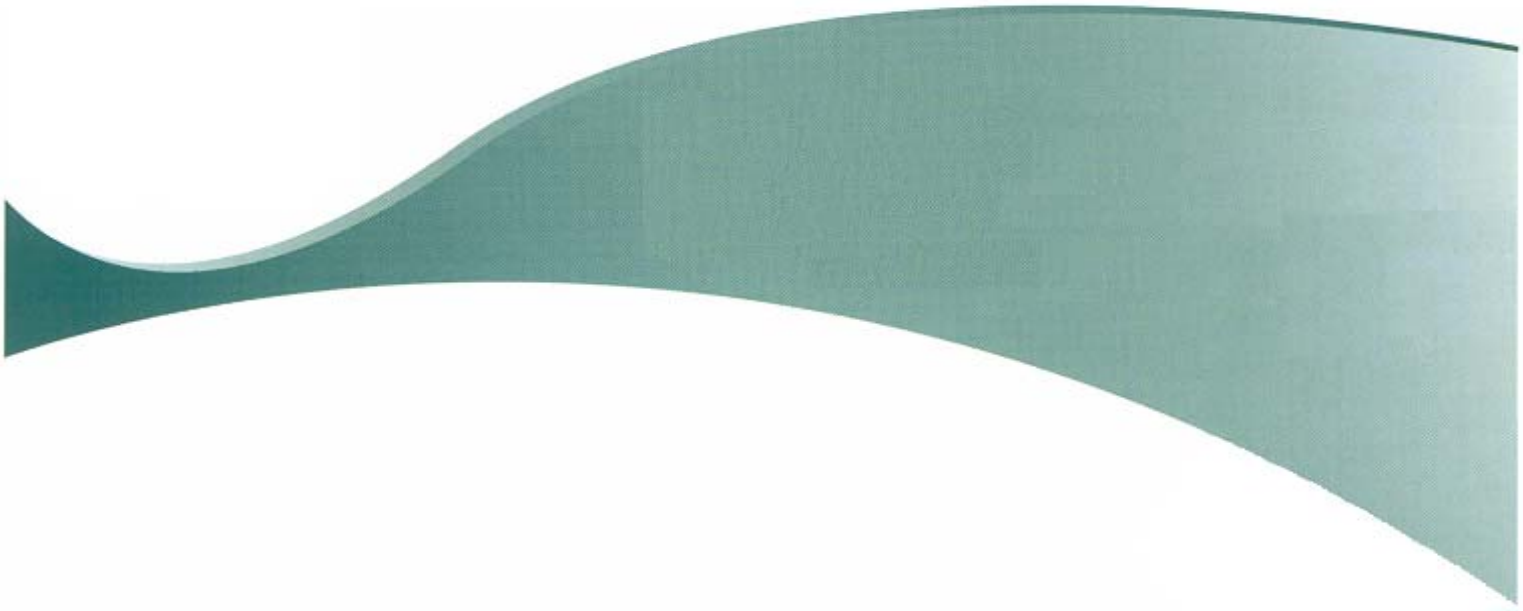
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Electronic Communications 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 Electronic Communications Policy.
Purpose:	To provide clear guidance on the appropriate, safe and legal way in which to use the HSE's electronic communications, email, internet and facsimile (fax) services.
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 electronic communications, email, internet and facsimile (fax) services.
Superseded Documents:	All local email, internet/intranet and fax policies and procedures.
Related Documents:	HSE Information Security Policy. HSE Information Technology Acceptable Use Policy. HSE Password Standards Policy. HSE Encryption Policy. HSE Internet Content Filter Standard. 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 electronic communications, email, internet and facsimile (fax) services in support of its administrative and service functions.

The inappropriate use of HSE' electronic communications, email, internet or fax services could expose the organization to risks ranging from virus attacks, theft and disclosure of information, disruption of network systems and services and litigation. The purpose of this policy is to define acceptable use of HSE's electronic communications, email, internet, intranet and fax services.

This policy is mandatory and by using any of the HSE's electronic communications, email, internet, intranet and fax services, 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 may be developed at a local level. The policy applies to:

- All electronic communications, email, internet, intranet and fax services provided by the HSE;
- 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 electronic communications, email, internet and facsimile (fax) facilities;
- All use (both personal & HSE business related) of the HSE's electronic communications, email, internet and facsimile (fax) facilities;
- All connections to (locally or remotely) the HSE's email, internet, intranet and fax facilities;
- 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 HSE's electronic communications, email, internet and facsimile (fax) services is based on the following principles:

- Access to the HSE's email and internet facilities should be regarded as a business requirement and not an automatic entitlement.

- Users have a responsibility to ensure that they use HSE's email, internet, intranet and fax facilities at all times in a manner which is lawful, ethical and efficient.

- Users are expected to respect the rights and property of others, including privacy, confidentiality and intellectual property.

- Users are expected to respect the integrity and security of the HSE's email, internet, intranet and fax facilities.

4.2 Monitoring

- The HSE reserves the right to routinely monitor, log and record any and all use of its electronic communications, email and internet facilities 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 electronic communications, email and internet activity 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 is not limited to details of internet sites visited, time spent on sites, pages viewed, information downloaded and the contents of email messages.

- 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 data under the *Data Protection Act 1988 & 2003.* Personal 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 electronic communications, email, internet, intranet and fax services 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 electronic communications, email, internet, intranet and fax services.

4.4 File Transfer

- Where possible all external transfers of confidential or restricted information must take place electronically via secure channels (i.e. Secure FTP, TLS, VPN etc) or encrypted email.

4.5 Email

- The primary purpose of the HSE email system is to promote effective communication on HSE business matters. Authorised users may be granted access to email services subject to the requirements of their role within the HSE.

- Users must respect the privacy of others at all times and only use email accounts that have been issued to them.

- Users who use the email system for personal use must ensure they present their communications in such a way that it is clear to the recipient that the email is of a personal nature and is not a communication on behalf of the HSE.

- Users should be careful when using their HSE email account to send personal messages that their words or actions do not have a negative impact on the HSE in any way.

- Only email facilities provided by the HSE may be used in connection with an individual users work for the HSE. The use of third party web based email services for the transmission of HSE confidential or restricted information is strictly prohibited.

- Access to third party web based email servers is not allowed using the HSE network. However email messages can be sent from the HSE network to third party web based email servers, but it should be noted that this is not a secure method of sending information.

- Where necessary individual users may apply for and be granted access to individual governmental or health sector web mail servers (i.e. Department of Health & Children, Royal College of Surgeons, voluntary hospitals etc.). In addition users who are on secondment to the HSE or are employed jointly by the HSE and another organisation (i.e. joint appointments) may apply for and be granted access to the web mail server of the organisation they are on secondment from or the organisation which they are a jointly employed by.

- Users who are secondment to the HSE from an academic institute or are jointly employed by the HSE and an academic institute will only be granted access to the academic institute's faculty web mail server. Access to the academic institute's student web mail servers is not permitted.

- For security reasons users who regularly receive HSE confidential or restricted information via email must not forward their HSE email messages to their own personal third party web based email account.

- Users should ensure they keep their personal email messages separate from their HSE business related email messages.

- In circumstances where it is necessary to transmit confidential or restricted information via email the sender must ensure the following checks are carried out before sending the information:

    1) The name and email address of all the intended recipient(s) are correct;

    2) The email message is clearly marked as "Private & Confidential";

    3) Only the minimum amount of confidential or restricted information as is necessary for a given function(s) to be carried out is to be sent;

- Where it is necessary to transmit confidential or restricted information to an email address outside of the HSE domain (i.e. one that does **not** end in "@hse.ie") the sender must ensure the following additional checks are carried out before and after sending the information:

    1) The transfer of the information is legally justifiable in accordance with the *Data Protection Acts 1988 and 2003.* If the sender is unsure about this they should the HSE Consumer Affairs department;

    2) The transfer is authorised by a HSE line manager (at grade 8 level or above). The authorisation must be issued in advance of the first instance and will apply thereafter if necessary.

    3) All confidential or personal information sent with the email message is encrypted inline with the requirements of the *HSE Encryption Policy* (*http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Encryption_Policy.pdf*)

    4) The password used to decrypt (read) the confidential or restricted information must not be sent along with the original email message.

5) Where practical check that the email message and information have been received by the intended recipient(s) (i.e. ask for a delivery receipt or phone the intended recipients to confirm receipt).

- Where there is a business need, HSE line managers may apply to the ICT department to have a generic or group HSE email address created which will be shared by multiple users (see section 4.3.3 of the *HSE Access Control Policy*).

- Users who require their secretaries or other colleagues to have access to their mailbox or calendars should setup shared mailboxes and calendars as necessary, rather than sharing their usernames and passwords.

- Email distribution lists must only be used for the authorised distribution of HSE work-related information which is relevant to everyone on the list.

- Email carries the same legal status as other written documents and should be used with the same care. Electronic communications maybe subject to *Freedom of Information Acts 1997 and 2003* and therefore available for public distribution.

- Email is capable of forming or varying a contract in the same way as a written letter. Users must be careful when wording an email, so it cannot be construed as forming or varying a contract when this is not the intention.

- A disclaimer must be automatically attached to all HSE out-going email messages. This disclaimer does not excuse the user from undertaking fundamental checks before sending the email (.i.e. checking the email content for accuracy, correct address etc.).

- The amount of email in a user's personal inbox and sent items folder must be kept to a minimum. Personal emails and attachments that are not HSE business related must be deleted as soon as possible after receipt. Confidential and restricted information which has been received via email should not be stored permanently in a user's mailbox once it has been read. Where practical the information should be transferred to a secure folder on a HSE server and deleted from the user's mailbox. Users should also empty the contents of the deleted items folder to ensure all local copies of the information have been deleted from their mailbox. Old HSE work-related email and attachments that are no longer required should be deleted and those that need be retained should be archived or moved to a personal folder on the users computer.

- During planned periods of absence such as career breaks, holidays or on training courses users should ensure where practical, their mailbox is put on divert to one of their colleagues 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 divert their mailbox to one of their 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 (For example the detection and prevention of fraud).

- Users leaving the employment of the HSE must ensure they forward on all important HSE business related email messages to their line manager or work colleagues before they leave so that there is no disruption to service delivery after they leave. They should also ensure they remove or delete all personal email messages (i.e. email messages which are of a personal nature and are not HSE business related) from their HSE mailbox before they leave as it may not be possible to get a copy of these once they have left the HSE.

- All email accounts maintained on the HSE's email system are the property of the HSE.

4.6 Internet & Intranet

- The primary purpose of the HSE internet and intranet service is to provide access to a valuable business tool to facilitate communication, information sharing, education and learning and authorized research.

- Authorised users may be granted access to internet services over the HSE network subject to the requirements of their role within the HSE.

- In accordance with the HSE *Internet Content Filter Standard* each user who has been granted access to the internet over the HSE network will be assigned to one or more HSE internet user access groups depending on their role or function within the HSE *(http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Internet_Content_Filter_Standard.pdf).*

- The HSE automatically filters internet access over its network and blocks access to individual websites or categories of internet content that it considers inappropriate.

- Users who have a legitimate HSE business reason may with the approval of their line manager (at grade 8 level or above) apply to their local ICT department for access to blocked internet content. Access requests should be made using the *HSE Internet Content Filter Exemption Request Form* (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Internet_Content_Filter_Exemption_Request_Form.pdf).*

- HSE line managers approving internet access requests of behalf of users have a responsibility to ensure they only approve and sign access requests for the user once they are satisfied that all categories and subcategories of internet content requested by the user are appropriate, necessary and relevant to the users current role within the HSE.

- Internet access from HSE smart devices will be exempt from the standard HSE internet content filtering protocols. However the users of HSE smart devices will be held responsible for all internet connections made from their HSE smart device. They must ensure that all internet access from their device is in accordance with requirements of this policy, the *HSE I.T. Acceptable Use Policy and the HSE Internet Filter Standard*.

- Confidential or restricted information regarding HSE business practices and procedures or personal information about any HSE patients, clients or employees should not be published on the HSE internet site (*www.hse.ie*) or intranet site (*http://hsenet.hse.ie/*).

- Users must not install or use any third party internet facilities on HSE computer devices without the prior authorization of their line manager and the ICT Directorate.

- Users must only use internet accounts that have been issued to them.

- Users need to remember that when visiting an internet site the unique address for their HSE computer device (i.e. I.P. address) can be logged by the internet sites that they visit so the HSE could be identified. Therefore any internet activity that is carried out by them may affect the HSE.

- The HSE will not be held liable for any financial or material loss by an individual user while accessing the internet for personal use.

- Users should be aware that information hosted on the internet offers no guarantee of accuracy, reliability or authenticity.

- The ICT Directorate on behalf of the HSE reserves the right to temporarily withdraw internet/intranet services or parts of the internet/intranet service for technical or operational reasons.

4.7 Social Media

- Access to most social media websites is blocked automatically by the HSE. However users who have a legitimate HSE business reason may with the approval of their line manager (at grade 8 level or above) apply to their local ICT department for access to these sites. Access requests should be made using the

HSE Internet Content Filter Exemption Request Form (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Internet_Content_Filter_Exemption_Request_Form.pdf*).

- Users should be aware that all use of social media, either in a personal capacity or when communicating on behalf of the HSE must be in accordance with the *HSE Social Media Policy & Guidelines* (*http://www.hse.ie/eng/staff/Resources/socialmedia/SocialandDigitalMediaPolicy%20and%20Guidance%20for%20HSE%20Employees.pdf*).

- Confidential or restricted information regarding HSE business practices and procedures or personal information about any HSE patients, clients or employees must not be posted or discussed on any social media websites.

4.8 Fax

- Users must respect the privacy of others at all times and only access fax messages where they are the intended recipient or they have a valid HSE work-related reason.

- Users who receive fax messages where they are not the intended recipient must contact the sender and notify them of their error and destroy or return the fax message as directed by the sender.

- Users need to consider whether a fax is the most appropriate means of communication. Confidential and personal information should not be transmitted by fax. Where possible the information must be encrypted and transmitted via email. However the following circumstances exist where it maybe acceptable to transmit confidential and personal information by fax:

    1) **Informed Consent:** All persons identified in the fax message have fully understood the risks and agreed;

    2) **No Alternative:** There are no other means available;

    3) **Medical Emergency:** Where a delay would cause harm to a patient/client/employee or the potential risk to a patient/client/employee is greater harm than the risk of disclosure of their personal information.

    4) **Legal Obligation:** A legal requirement exists to fax such data.

- In circumstances where it is necessary to fax confidential or restricted information the sender must ensure the following checks are carried out before and after faxing the information:

1) The fax message includes a ***HSE Fax Cover Sheet*** (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/*);

2) The fax number of the intended recipient(s) is correct.

3) Only the minimum amount of confidential or restricted information as is necessary for a given function(s) to be carried out is included in the fax message;

4) Where practical telephone the intended recipient before the transmission to ensure they are waiting by the fax machine for the fax message;

5) When the fax message has been sent, keep a copy of the transmission slip and where practical contact the intended recipient to confirm receipt of the fax message.

6) Remove all documents from the fax machine immediately after faxing.

- Where possible, fax machines which are used to send or receive confidential fax message's should be physically secured and positioned in such a way as to minimise the risk of unauthorised individuals accessing the equipment or viewing any incoming messages. Wherever possible the fax machine should be switched off outside of normal office hours.

- Where possible, only fax machines which are owned or leased by the HSE should be used to send or receive confidential and restricted information.

- All transfer of confidential or restricted information via fax message to third parties must be authorised by a HSE line manager (at grade 8 level or above). The authorisation must be issued in advance of the first instance and will apply thereafter if necessary.

- Users who frequently send confidential or restricted information via fax to third parties should periodically remind the third parties that they need to notify the HSE immediately if their fax number(s) changes.

- Fax messages are capable of forming or varying a contract in the same way as a written letter. Users must be careful when wording a fax message, so it cannot be construed as forming or varying a contract when this is not the intention.

- Fax messages carry the same legal status as other written documents and should be used with the same care. Fax communications maybe subject to *Freedom of Information Acts 1997 and 2003* and therefore available for public distribution

4.9 Security

- Users who breach information security by inadvertently transmitting confidential, restricted or personal information by fax, email or the internet to an incorrect address or destination, must follow the procedure below:

    1) The breach must be managed and reported 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*);

    2) The user must contact the recipient of the fax, email or internet message immediately and request that the information is returned to the HSE immediately or destroyed.

- Viruses and other forms of malicious software are usually spread via email and the internet. Users who receive a virus warning message must notify the ICT Directorate and under no circumstances should they forward it on to other users.

4.10 Unacceptable Use

- The HSE's email, internet and fax facilities may 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 purposes, 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 enter into contractual agreements inappropriately (i.e. without authorisation or where another form of agreement is required);
    6) For any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);
    7) To send messages that contain libelous, defamatory or harassing remarks, images or other material;
    8) To bully others;
    9) For creating or transmitting "junk" or "spam" emails. This includes but is not limited to unsolicited commercial emails, jokes, chain-letters or advertisements;

10) For any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law;
11) For any activity that would deliberately compromise the privacy of others;
12) For any activity that would intentionally waste the HSE's resources (e.g. employee time and IT resources);
13) For any activity that would intentionally compromise the security and availability of the HSE's IT services (e.g. by deliberately or carelessly causing computer virus and malicious software infection);
14) To transmit confidential or personal information outside the HSE unless the information has been encrypted (email and internet) and the transmission has been authorised by a HSE line manager (at grade 8 level or above);
15) 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;
16) To forge or attempt to forge an email message or, send an email message using another persons account without their permission;
17) To upload or download access-restricted HSE information contrary to this policy or in violation of any other HSE policy.

- The above list should not be seen as exhaustive, as other examples of unacceptable use of the HSE's electronic communications, email, internet and facsimile (fax) services may exist.
- The HSE has the final decision on deciding what constitutes excessive personal use.
- The HSE will refer any use of its electronic communications, email, internet and facsimile (fax) services for illegal activities to the Gardai

5.0 Roles & Responsibilities

5.1 ICT Directorate

The ICT Directorate is responsible for:

- The provision of reliable and secure email and internet facilities;
- The deployment and management of internet content monitoring and filtering facilities;
- The deployment and management of appropriate technical and security safeguards to ensure availability, integrity and security of the email and internet facilities;

- The provision, deployment and management of encryption facilities;
- The provision of training, advice and guidance to computer systems users;
- Monitoring of all electronic communications, email and internet traffic on behalf of the HSE.

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 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 related 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 they only approve and sign internet access requests for employees, once they are satisfied that all categories and subcategories of internet content requested by the employee are appropriate, necessary and relevant to the employees current role within the HSE.

- Reporting all actual or suspected breaches of information security 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 electronic communications, email, internet and facsimile(fax) services 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 they process at all times;

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

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

5.5 Information Security Project Board (ISPB)

The ISPB is responsible for:

- Setting the *HSE Internet Content Filter Standard (http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Internet_Content_Filter_Standard.pdf)*.

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 electronic communications, email, internet and facsimile (fax) services 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 that 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 intranet at – (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/*)

Appendix A

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

Breach of Information Security: The situation where HSE confidential or personal 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

Decryption / Decrypt: The process of decoding information which has been converted into an unreadable form (cipher text) back into a readable form (plain text).

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

Email: System for sending messages electronically from one individual to another via telecommunications links between computers.

Email Disclaimer: Legal statement appended to an email message.

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.

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 computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, 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

Internet: A worldwide computer network consisting of smaller networks which facilities the transmission and exchange of information for commercial, educational and governmental purposes 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.

Personal Use: The use of the HSE's Information Technology (IT) resources for any activity(s) which is not HSE work-related.

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

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.

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 personal information (i.e. mental health status, HIV status, STD/STI status etc)
- Childcare / Adoption information
- Social Work information
- Addiction Services information
- Disability Services information
- Unpublished financial reports
- Strategic corporate plans
- Sensitive medical research

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

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 Web Based Email Services (Servers): Any internet accessible email facilities which are not managed or hosted by the HSE. Including both commercial email services (for example, Microsoft Hotmail, Yahoo Mail, GMail (Google Mail), AOL Mail, eircom email, Indigo email and Mail.Com. etc) and non-commercial (for example, third level training and educational institutions etc).

Third Party Internet Facilities: Any internet facilities which are not managed or provided by the HSE. These include those provided directly by an Internet Service Providers (ISP). For example Eircom, ESAT BT, Irish Broadband, Smart Telecom, Clearwire, Broadband4Ireland, Chorus NTL and UTV etc.

Transmission / Transmitted / Transfer: The process of sending or moving something (information or otherwise) from one location to another location.

Users: Any authorized individual who uses the HSE's electronic communications, email, internet, intranet and fax services.