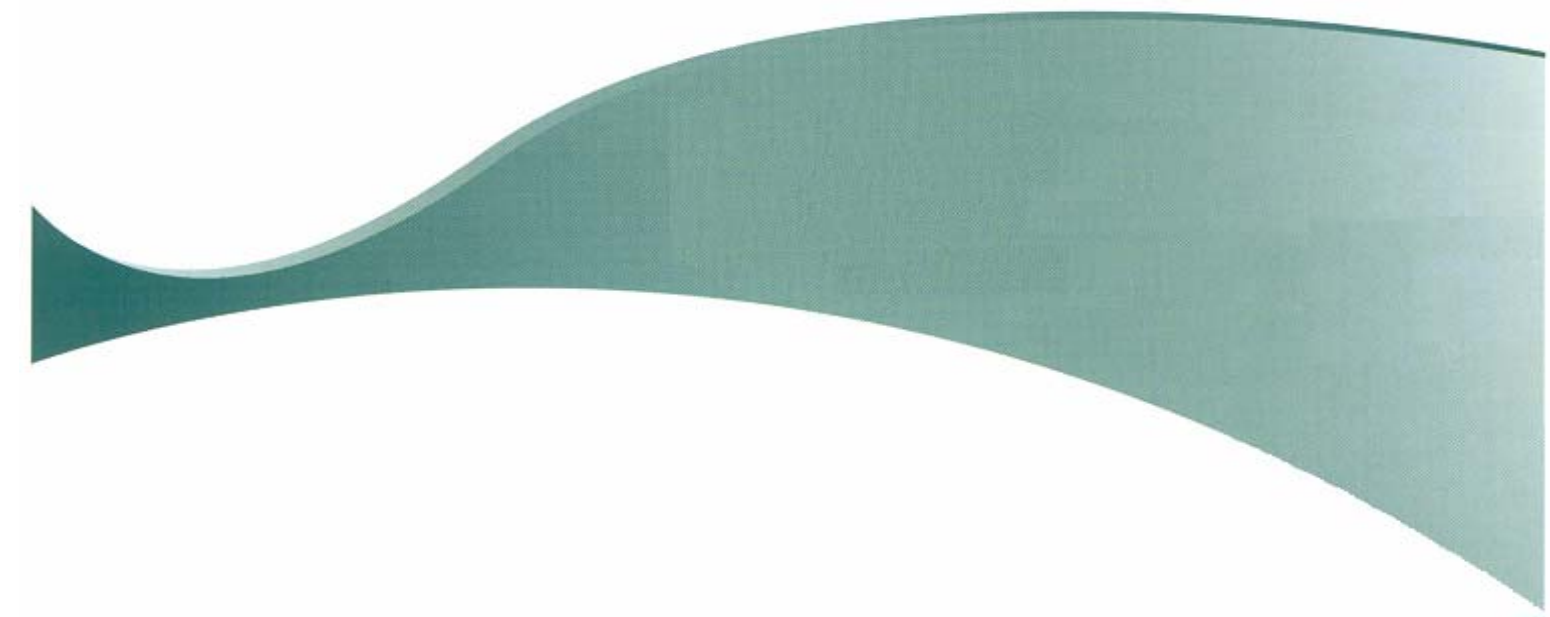
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Mobile Phone Device Policy



Version 2.0

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 Mobile Phone Device Policy.
Purpose:	To define the acceptable use and management of HSE mobile phone devices.
Author:	ICT Directorate on behalf of the HSE.
Publication date:	November 2010
Target Audience:	All employees, clients and third parties that use HSE mobile phone devices.
Superseded Documents:	All local mobile phone policies.
Related Documents:	HSE National Financial Regulations. HSE Electronic Communications Policy. HSE Password Standards Policy. HSE Encryption Policy. HSE Information Technology Acceptable Use Policy. HSE Data Protection Breach Management Policy.
Review Date:	November 2011
Contact Details:	Chris Meehan ICT Directorate, Dr.Steevens Hospital Steevens Lane Dublin 8 Email: chris.meehan@hse.ie Helen Lambert ICT Directorate Lackin Kilkenny Email: helen.lambert@hse.ie

1.0 Purpose

The Health Service Executive (HSE) is committed to the correct and proper use of mobile phone devices in support of its administrative and service functions.

The inappropriate use of mobile phone devices could expose the HSE to risks including, theft and / or disclosure of information, disruption of services, fraud or litigation. The purpose of this policy is to define acceptable, safe and secure standards for the use and management of mobile phone devices within the HSE.

This policy is mandatory and by using any mobile phone devices 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 and procedures which are developed at a local level. The policy applies to all mobile phone devices which are owned or leased by the HSE, users and, holders of these mobile phone devices and, all use of such mobile phone devices.

The financial, management and reporting elements of this policy are based on the ***HSE National Financial Regulations (NFR)*** which available on the HSE intranet (*http://hsenet.hse.ie/HSE_Central/finance_Transformation_Projects/Financial%20Regulations/*).

All exceptions to this policy must be authorised by the National Director for Finance. Exception requests must be submitted in writing using the ***HSE IT Security Policy & Procedures Exception Request Form*** (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/IT_Security_Policy_Exception_Request.pdf*).

3.0 Definitions

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

4.0 Policy

4.1 Assignment & Approval of Mobile Phone Devices

- The relevant senior manager (Assistant National Director (or equivalent) level or higher) must approve the assignment of a HSE mobile phone device or may, by formal written decision, nominate a member(s) of their management team who will have authority to approve the assignment of mobile phones on their behalf. Nominees in this regard must be at Grade VIII level or higher and a copy of the decision must be forwarded by the senior manager to the relevant management team member and relevant Assistant National Director of Finance.

- The senior manager or his/her nominee approving the assignment of a HSE mobile phone device must ensure that the necessary budgetary provision has been made for the initial and ongoing costs related to the use a mobile phone device.

- HSE Mobile phone devices maybe assigned on an 'individual' basis for use by a designated employee or on a 'shared basis' for use by a designated HSE directorate or service area.

- The assignment of a HSE mobile phone device must be made for an initial two year term. At the end of the two year term, the need for the mobile phone device must be reviewed by the relevant senior manager or their nominee.

4.2 Criteria for determining the assignment of a HSE mobile phone device

- The decision to approve the assignment of a HSE mobile phone device to an employee must only be made after careful consideration and examination of the employee's duties. A HSE mobile phone device must only be issued to employees who meet at least one of the following criteria.

    a) The employee's duties require them to spend time out of the office or normal place of work;
    b) The employee is on an official on-call rota;
    c) The employee has been identified as a key member of staff and needs to be contactable at any time;
    d) The employee's duties are such that the mobile phone device is needed for health and safety reasons;
    e) At the discretion of the Chief Executive Officer.

- Once a decision has been made to assign a HSE mobile phone device, the senior manager or their nominee must forward a written copy of decision to the relevant Assistant National Director of Finance.

4.3 Local Mobile Phone Device Administrator

- The budget holder within each HSE directorate or service area must nominate a member of their staff who will act as a local mobile phone device administrator and be responsible for dealing with all administrative matters relating to usage of mobile phone devices within their area of responsibility.

- The budget holder must ensure that the relevant Assistant National Director of Finance and all employees within their directorate or service area are notified (in writing or via email) of the name and contact details of the local mobile phone device administrator.

- The local mobile phone device administrator must ensure that a copy of this policy has been issued to each employee and the employee has signed a copy of the ***HSE Mobile Phone Device User Agreement*** - (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Po*

licies_and_Procedures/Forms/) in advance of them receiving their HSE mobile phone device.

4.4 Procurement of mobile phone devices

- All HSE mobile phone devices and associated equipment (e.g. car kit, battery charger etc) must be purchased in line with National HSE procurement contracts. The contact details for all current contacted mobile phone service providers can be obtained from the HSE Procurement Directorate.

- Only HSE mobile phone devices which have been purchased in line with National HSE procurement contracts or through the ICT Directorate approved channels will be allowed connection to the HSE network.

- All HSE mobile phone devices, associated equipment and mobile phone accounts remain the property of the HSE.

4.5 Register of Mobile Phone Devices

- Each local mobile phone device administrator must prepare and maintain (in electronic format) a list of all mobile phone devices within their area of responsibility. The list must include the following information for each mobile phone device:

    a) Assignment details (Employee name, location, contact details, grade, directorate/service and email address);
    b) Mobile phone device telephone number;
    c) Decision number & date authorizing assignment of mobile phone device;
    d) Date the mobile phone device was issued;
    e) PIN & PUK number;
    f) Billing address and contact name;
    g) Delivery address if different from above;
    h) Contact details (Name, location, grade/title, directorate/service, email address and contact telephone number(s)) of line manager responsible for reviewing and approving employees mobile phone device bills;
    i) Dates and details of any upgrades or replacements;
    j) Dates and details of any associated equipment (e.g. car kit, battery charger etc) supplied with the mobile phone device;
    k) Details of any restrictions applied;
    l) Review date.

4.6 Mobile phone device billing

- Local mobile phone device administrators must ensure that individual mobile phone device invoices along with the ***HSE Mobile Phone Declaration Form*** - (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/*) are sent each month to the assigned user of a HSE mobile phone device, for sign-off before payment.

- The user of the mobile phone device must identify and quantify all personal call charges and costs on the invoice and, return this along with the signed ***HSE Standard Declaration Form*** to their local mobile phone device administrator for payment processing.

- All personal call charges and costs must be reimbursed to the HSE by the user in accordance with the ***HSE National Financial Regulations.***

4.7 Monitoring

- Individual budget holders must implement local procedures to monitor mobile phone usage within their directorate or service to ensure compliance with this policy.

- The HSE reserves the right to monitor, capture and inspect any phone call information made on a HSE mobile phone device or on a HSE mobile phone account, in order to:

    a) Investigate system problems;
    b) Investigate potential security violations;
    c) Maintain system security and integrity;
    d) Prevent and detect misuse;
    e) Review expenditure charged to a mobile phone device telephone account with a view to seeking reimbursement from HSE employees in respect of all costs relating to the personal usage of their HSE mobile phone device;
    f) Ensure compliance with HSE policies, current legislation and applicable regulations.

- While the HSE does not routinely monitor an individual user's mobile phone device activity, it reserves the right to do so when a breach of its policies or illegal activity is suspected. This monitoring may include but is not limited to details of telephone calls made, messages and emails sent to and from the device, internet access and information stored on the mobile phone device.

- The monitoring of an individual user's mobile phone device activity must be authorised by the HR Directorate and the individuals line manager (General Manager level or above). The results of all monitoring will be stored securely and will only be shared with those authorised to have access to such information.

4.8 Usage

- HSE mobile phones devices are to be used primarily for HSE work-related purposes. Occasional and limited personal use maybe permitted, provided that all personal call charges and costs are identified, quantified, and reimbursed to the HSE.

- Mobile phone devices may only be used by an assigned HSE employee and must not be used by any other HSE employees or third parties without the prior authorization of the local mobile phone device administrator.

- Users must ensure that they use HSE mobile phone devices at all times in a manner which is lawful, ethical and efficient. The HSE may withdraw a mobile phone device from any employee who it believes is not complying with this policy or who misuses a mobile phone device in any manner.

- Users must make every reasonable effort to ensure that their HSE mobile phone device is secured at all times, kept charged and switched on during working hours.

- Only software which has the correct and proper license and has been purchased and/or approved by the ICT Directorate may be installed and used on a HSE mobile phone device.

4.9 Restrictions on Usage

- Calls made from a HSE mobile phone device must be restricted to local and national phone numbers only (i.e. calls to telephone numbers inside the Republic of Ireland/Northern Ireland). The use of mobile phone devices to make international calls (i.e. calls to telephone numbers outside the Republic of Ireland/Northern Ireland) is prohibited except in exceptional circumstances such as when:

    a) A user is out of the country on official HSE business.
    b) A user is working off-site or out of hours and needs to contact an external service provider / consultant based abroad.
    c) In case of an emergency.
    d) Or at the discretion of the relevant senior manager or the CEO.

- HSE mobile phone devices must not be used to dial premium rate numbers (i.e. calls to telephone numbers beginning with the 15xx prefix – i.e. 1550, 1590 etc).

4.10 Email & Internet

- Where a mobile phone device is capable of allowing email and/or internet access, all use of these facilities on the mobile phone device is governed by the terms 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 Health & Safety

- For legal reasons and in the interest of public and personal safety, the use of HSE mobile phone devices within a vehicle must be in accordance with the relevant legislation. The *Road Traffic Act 2006* makes it an offence for a driver of a vehicle to hold a mobile phone device while driving the vehicle.

The offence is 'holding' a mobile phone device and does not require the driver to be making or receiving a call but merely holding the phone. The *Act* defines 'holding' as holding the mobile phone device by the hand or supporting or cradling it with another part of the body. The use of hands-free phone kits or Bluetooth technology is not an offense under the *Act*.

- The use of a mobile phone device within HSE premises and other clinical/medical facilities should be checked before use for fear of interference with sensitive electronic medical equipment.

4.12 Security

- Users must ensure their HSE mobile phone device is protected at all times. As a minimum all mobile phone devices must be protected by the use of a Personal Identification Number (PIN). Where it is technically possible the mobile phone device must be password protected and all passwords must meet the requirements of ***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****).***

- Users must take all reasonable steps to prevent damage or loss to their mobile phone device. This includes not leaving it in view in an unattended vehicle and storing it securely when not in use. The user may be held responsible for any loss or damage to the mobile phone device, if it is found that reasonable precautions were not taken.

- Confidential and personal information must not be stored on a HSE mobile phone device without the prior authorization of the HSE information owner. Where confidential and personal information is stored on a HSE mobile phone device, the information must be encrypted in accordance with the ***HSE Encryption Policy*** *(http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Encryption_Policy.pdf)*

4.13 Confidentiality & Privacy

- In view of the need to observe confidentiality at all times, users must be vigilant when using their HSE mobile phone device in public places in order to avoid unwittingly disclosing sensitive employee, patient or client information.

- Users must respect the privacy of others at all times, and not attempt to access HSE mobile phone device calls, text messages, voice mail messages or any other information stored on a mobile phone device unless the assigned user of the device has granted them access.

- Mobile phone devices equipped with cameras must not be used inappropriately within the HSE. In this regard users must not:

a) Take photographs or video recordings using a HSE mobile phone device or any other device in areas where an employee, patient or client has a reasonable expectation of privacy.

b) Distribute photographs, videos or recordings of any type using HSE mobile phone devices around the HSE, unless the content and use have been approved in advance by the user's line manager.

- Users must not use their HSE Mobile phone device to send text messages which contain any confidential and/or personal information regarding the HSE, its employees, clients or patients.

- All email messages sent from a HSE mobile phone device which contain confidential and/or personal information must be sent and encrypted in accordance with 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) and the* ***HSE Encryption Policy*** ***(****http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Encryption_Policy.pdf)*

4.14 Lost or stolen mobile phone devices

- Users must report all lost or stolen mobile phone devices to their line manager and their local mobile phone administrator immediately.

- Local mobile phone administrators must report the incident to their senior manager, the mobile phone service provider and the relevant Assistant National Director of Finance immediately.

- Incidents where a lost or stolen HSE mobile phone device contained confidential or personal information must be reported and 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/*).

4.15 Employees Leaving the HSE / Employee Transfers

- Employees must return their HSE mobile phone device and any associated equipment (e.g. car kit, battery charger etc) to their local mobile phone device administrator before they leave the employment of the HSE.

- Employees transferring internally within the HSE must ensure that they notify the local mobile phone device administrators in the area they are leaving and area they are joining to ensure amendments are made to the register of mobile phone devices.

- Employees who are retiring / resigning may, by agreement, purchase their mobile phone and any associated equipment (e.g. car kit, battery charger etc)

that may have been provided, from the HSE for their current value. The current value of the mobile phone device and associated equipment will be set by the National Director of Finance.

4.16 Disposal of Mobile Phone Devices

- Old and obsolete HSE mobile phone devices must be recycled in accordance with the requirements of the *Waste Electrical and Electronic Equipment (WEEE)* directive.

4.17 Unacceptable Use

HSE mobile phone devices may not be used:

- For excessive personal use;
- For commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
- For political activities; such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions;
- To knowingly misrepresent the HSE;
- To transmit confidential or personal data outside the HSE unless the data has been encrypted and transmission has been authorised by the data owner and Consumer Affairs;
- To send text messages which contain any confidential and/or personal information regarding the HSE, its employees, clients or patients;
- To enter into contractual agreements inappropriately (i.e. without authorisation or where another form of agreement is required);
- To view, create, download, host or transmit (other than for properly authorised and lawful purposes) pornographic, offensive or obscene material(i.e. information, images, vide clips, audio recordings etc), which could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs;
- To retrieve, create, host or transmit any material which is designed to cause annoyance, inconvenience or needless anxiety to others;
- To retrieve, create, host or transmit material which is defamatory;
- For any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);
- For any activity that would compromise the privacy of others;
- For any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to the HSE or others;
- For any activity that would intentionally waste the HSE's resources (e.g. employee time and IT resources);

- For any activity that would intentionally compromise the security of the HSE's IT resources, including the confidentiality and integrity of data and availability of IT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection);
- For the installation and use of software or hardware tools which could be used to probe, and / or break the HSE IT security controls;
- 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;
- For creating or transmitting "junk" or "spam" emails. This includes unsolicited commercial emails, chain-letters or advertisements;
- For any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law.

This should not be seen as an exhaustive list. Other examples of unacceptable use of HSE mobile phone devices may exist.

5.0 Roles & Responsibilities

5.1 Assistant National Director of Finance

The relevant Assistant National Director of Finance is responsible for:

- Ensuring that there is centralised visibility of:

    a) The assignment of HSE mobile phone devices:
    b) The replacement and upgrade of HSE mobile phone devices;
    c) The restrictions on the usage of HSE mobile phone devices (see 4.9).

5.2 Senior Managers

Senior Managers (or their nominee) are responsible for:

- The implementation of this policy and all other relevant policies within the directorate or service for which they are responsible;
- Ensuring adequate procedures are in place for approving and renewing the assignment of mobile phone devices for employees within their directorate or service area;
- Ensuring HSE mobile phone devices are only assigned to employees that satisfy the approved criteria (see section 4.2);
- Forwarding copies of decisions assigning mobile phones to the relevant Assistant National Director of Finance.

5.3 Budget Holders

The budget holder within a HSE directorate or service area is responsible for:

- Ensuring that all mobile phone device costs incurred within their directorate or service area are:

    a) Necessary for the service;
    b) Represent value for money;
    c) Are appropriately monitored and controlled;

- Implementing procedures within their own area of responsibility to ensure that all personal call charges and costs are identified and reimbursed to the HSE;

- Nominating a member of their staff who will act as a local mobile phone device administrator;

- Keeping the relevant Assistant National Director of Finance informed of the contact details of the local mobile phone administrator within their directorate or service.

5.4 Local Mobile Phone Device Administrators:

Each local mobile phone device administrator is responsible for:

- Dealing with all administrative matters relating to the usage of mobile phone devices within there directorate or service area;

- Ensuring that employees receive a copy of this policy and sign a copy of the ***HSE Mobile Phone Device User Agreement*** in advance of them receiving their HSE mobile phone device;

- Maintaining signed copies of all ***HSE Mobile Phone Device User Agreements*** for their directorate or service area;

- Preparing and maintaining (in electronic format) an up to date list of all mobile phone devices and associated equipment (e.g. car kit, battery charger etc) within their directorate or service area;

- Ensuring that individual mobile phone device invoices along with ***HSE Standard Declaration Form*** are signed off by the assigned user of each HSE mobile phone device within their directorate or service area;

- Ensuring all mobile phone devices and associated equipment (e.g. car kit, battery charger etc) are returned to them when an employee leaves the employment of the HSE or transfers to another HSE directorate or service area;

- Reporting all lost or stolen HSE mobile phone devices to the relevant people.

5.5 Users:

Each user assigned a HSE mobile phone device is responsible for:

- Ensuring that they use their HSE mobile phone device at all times in a manner which is lawful, ethical and efficient;
- Ensuring all call charges and costs associated with their personal use of the mobile phone device are identified, quantified, and reimbursed to the HSE.
- Taking appropriate precautions to ensure the security of their HSE mobile phone device and the information stored on the device;
- Complying with the terms of this policy and all other relevant HSE policies, procedures, regulations and applicable legislation;
- Complying with instructions issued in relation to mobile phone usage;
- Reporting all misuse and breaches of this policy to their line manager and their local mobile phone device administrator immediately;
- Reporting all lost or stolen mobile phone devices to their line manager and their local mobile phone administrator immediately;

5.6 National Procurement Directorate:

- Are responsible for ensuring that agreements or national contracts are in place for the procurement of mobile phone devices and associated equipment on behalf of the HSE.

6.0 Enforcement

- The HSE reserves the right to take such action as it deems appropriate against users who breach the conditions of this policy. HSE employees who breach this policy may be denied access to the organizations information technology resources, and 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, may lead to the withdrawal of HSE information technology resources to that third party and/or the cancellation of any contract(s) between the HSE and the third party.
- The HSE will refer any use of its mobile phone devices for illegal activities to the appropriate law enforcement agencies.

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 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.

Confidential Information: Information that is given to HSE in confidence and/or is not publicly known. The Information must only be accessible to those person(s) who are authorised to have access. For example – unpublished financial reports, tenders, contracts, unpublished research material, passwords etc.

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

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

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

Line manager: The individual a user reports directly to.

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

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

Mobile Phone Service Provider: The organization that operates and maintains a mobile telephone network. (For example Vodafone, O2, Meteor etc.)

Personal Information: Information relating to a living individual (i.e. HSE employee, client or patient) who is or can be identified either from the Information or

from the Information in conjunction with other information. For example: - an individuals name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.

Personal Use: The use of a HSE mobile phone device for any activity(s) which are not HSE work-related.

Personal Call: Telephone calls or text messages which are not HSE work-related.

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.

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 stick/keys, external hard drives.

Senior Manager: Any HSE employee at Assistant National Director, Regional Director of Operations (RDO), Hospital Network Manager, Local Health Office Manager, NHO Hospital Manager level or higher.

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.

Test Messages: Short messages which are sent in clear text from a mobile phone device to another mobile phone device using the Short Message Service (SMS).

Third Party(s): Any individual, consultant, contractor or agent not registered as a HSE employee.

Users: Any individual assigned the use of a HSE mobile phone device.