Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

HEALTH SERVICE EXECUTIVE

NATIONAL FINANCIAL REGULATION

MOBILE PHONE DEVICES

NFR - 27

Ver 2.0 4/5/2017

NFR – 27 Mobile Phone Devices

27.1	Introduction	*on page 3*
27.2	Purpose	*on page 3*
27.3	Scope	*on page 3*
27.4	Assistance/Further Information	*on page 3*
27.5	Effective Date	*on page 3*
27.6	Definitions	*on page 4*
27.7	Criteria for Determining the Assignment of a HSE Mobile Phone Devices	*on page 6*
27.8	Approval of assignment / upgrade / replacement of mobile phone devices	*on page 7*
27.9	Procurement of Mobile Phones Devices	*on page 7*
27.10	Usage Requirements and Restrictions	*on page 8*
27.11	Security	*on page 10*
27.12	Confidentiality and Privacy	*on page 10*
27.13	Procurement of Mobile Phones Devices	*on page 15*
27.14	Lost or stolen Mobile Phone Devices	*on page 11*
27.15	Employees Leaving the HSE / Employee Transfers	*on page 11*
27.16	Disposal of Mobile Phone Devices	*on page 11*
27.17	Roles & Responsibilities	*on page 12*
27.18	Monitoring	*on page 14*
27.19	Processing of Mobile Phone Device Bills	*on page 15*
27.20	Health and Safety	*on page 15*
27.21	Segregation of Duties	*on page 15*
27.22	Reporting of Irregularities	*on page 16*
27.22	Audit	*en page 16*

27.1. Introduction

27.1.1. The Health Service Executive (HSE) has responsibility for the stewardship and proper management of public funds granted to it for the provision of health and personal social services. Staff, in the performance of their duties, may be required to hold Mobile Phone Devices. 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.

27.2. Purpose

27.2.1. To document policies and procedures for the correct and proper use of Mobile Phone Devices.

27.2.2. 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

27.3. Scope

27.3.1. The policy applies to all mobile phone devices which are used by the HSE.

27.4. Assistance / Further Information

27.4.1. Additional information regarding this regulation should be addressed to the Assistant National Director of Finance, Annual Financial Statements (AFS) & Governance.

27.4.2. Requests for derogation from specified directives should be made in writing to the above Assistant National Director of Finance, and may be implemented only after written authorisation is received from said directorate.

27.4.3. It is intended that this regulation will be regularly updated to reflect and incorporate new and additional legislative and other directives. Notifications will be issued on HSE National Intranet - National Financial Regulations and via email communications.

27.5. Effective Date

27.5.1. This directive is effective immediately and supersedes all prior regulations/directives issued relating to mobile phone devices. HSE previous policy on this topic was the subject of NFR-01 Purchase to Pay, Chapter 4: Non Order Payments and the detailed national policy and procedures was documented in the appendices to that regulation.

27.6. Definitions

A list of terms used throughout this policy is defined below:

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

Incidental Usage: Incidental telephone usage refers to those calls which are unrelated to the conduct of official HSE business, but are authorised if they:

1. Do not adversely affect the performance of the duties of the employee or the employee's department; and
2. Are not for commercial purposes, for-profit activities unrelated to HSE, or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sales or supply of goods or services).
3. Are of a reasonable duration and frequency; and
4. Could not reasonably have been made at another time; and
5. Do not result in additional charges to HSE (e.g. long distance, premium calls/texts).

The following are examples of incidental telephone usage. These examples do not supersede any expanded local guidelines that might prohibit such use:

1. Calls to notify family members and/or physician in case of an emergency.
2. Calls to notify family members of work schedule changes, delays or changes in travel plans.
3. Brief local calls to an employee's residence, family member, child's school, child care provider, or elder-care provider.
4. Brief calls to local businesses (including government agencies, physicians or auto and home repair) that can only be reached during normal work hours.

Note: This list is not conclusive and is examples for guidance purposes only.

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 (IT) resources: Includes all computer facilities and equipment, networks and data communications infrastructure, telecommunications systems and equipment, internet and email facilities, software 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

Invoice: Mobile Phone Device Bill.

Mobile Computer Device: Any handheld computer device including but not limited to laptops, notebooks, tablet computers, PDA devices.

Mobile Phone Device: Any wireless telephone device not physically connected to a landline telephone system. Including but not limited to mobile telephones, Smartphone devices and 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 organisation that operates and maintains a mobile telephone network. (For example Vodafone, O2, Meteor etc.)

Local Mobile phone device Administrator: [1]Local officer responsible for dealing with all administrative matters relating to usage of mobile phone devices within their area of responsibility. The Local Mobile Administrator reports to a Regional Mobile Administrator on issues relating to Mobile Phone Devices.

National ICT Lead, Mobile Phone Devices: ICT Manager who leads the project working with Mobile Phone Service Providers, Regional Mobile Administrators, Procurement and Finance Department staff on the implementation of the award of the National Mobile Framework and on the adherence to HSE mobile policies/ mobile financial regulations.

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.

[1] In some locations this role of the local mobile phone device administrator is not assigned to local area management but is the function of the ICT department. References in this document to the local mobile phone device administrator may not be in the role of a local area officer but is assigned to an ICT officer's profile.

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.

Regional Mobile Administrator: Lead person within their region on all issues on Mobile Phone Devices. This person coordinates the work of the Local Mobile Administrators in relation to their work on Mobile Phone Devices and liaises with the National ICT Lead, Mobile Phone Devices to ensure implementation of the award of the National Mobile Framework and to ensure compliance with National Mobile policies within their region.

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, Hospital Network Manager, Local Health Office Manager, NHO Hospital Manager level or higher.

Senior Manager: Any HSE employee at Assistant National Director/Equivalent Grade.

System Administrators: The people responsible for the day to day management of HSE information systems and applications. 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(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.

27.7. Criteria for determining the assignment of a HSE mobile phone device

27.7.1. The decision to approve the issue of a mobile phone device to an employee should only be made after careful consideration and examination of the employee's duties.

27.7.2. A HSE mobile device must only be issued to employees who meet at least one of the following criteria;

1. The employee has been identified as a key member of staff and needs to be contactable at any time;
2. The employee's duties require them to spend time out of the office or normal place of work;
3. The employee's duties are such that the mobile phone device is needed for health and safety reasons;
4. The employee is on an official on-call rota;
5. At the discretion of the Director General (DG).

27.8. Approval of assignment / upgrade / replacement of mobile phone devices.

27.8.1. The individual and the their Line Manager must complete a 'Mobile Phone Device Application Form (Appendix A)[2] outlining the following:

1. Name, grade, title, service and address of staff member
2. Personnel Number
3. Email address and landline phone number of the staff member
4. Basis for requirement of the mobile phone device
5. Name, grade, title, service, email address, contact telephone number(s) and work location address of the line manager responsible for reviewing and approving the staff member's mobile phone device invoices
6. Name, grade, title, service, email address, contact telephone number(s) and work location address of the local mobile phone device administrator who is charged with the administrative matters on this phone. Each HSE local HSE office or 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. Refer Roles & Responsibilities.
7. Any exceptions required to the standard restrictions on mobile phone devices and justification for same.
8. Details of the device required and whether it's for the purposes of an upgrade or a replacement.

27.8.2. The form must be approved by the Line Manager.

27.8.3. All employees must receive a copy of this policy and confirm in writing that they have read same and declare their agreement to comply with said directives.

27.8.4. 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.

27.9. Procurement of mobile phones devices

27.9.1. The ICT directorate is responsible for managing and logging the procurement of mobile phone devices on behalf of the HSE.

27.9.2. 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.

27.9.3. Once the relevant forms has been completed and approved, it should be passed on to the local mobile phone device administrator who will forward on the request to their local ICT department and they will log the request for processing with the contracted mobile phone service provider.

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

---

[2] *The forms in this regulation may be amended to acquire compatibility with the relevant systems/service provider agreements, while ensuring that the details on the standard forms constitute the minimum data to be captured for the process. All forms should be printed out on official HSE letterhead paper. Refer http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/ for latest version of this form.*

27.10. Usage Requirements and Restrictions

27.10.1. HSE mobile phones devices are to be used for HSE work-related purposes. A taxable benefit will not be treated as arising where any private use is incidental.

27.10.2. Mobile phone devices are assigned to a position or function and not to individual; however the post holders name is supplied to the mobile phone device supplier.

27.10.3. The mobile phone device 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 authorisation of the local mobile phone device administrator.

27.10.4. 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.

27.10.5. 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.

27.10.6. 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.

27.10.7. 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's Electronic Communications Policy.

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

27.10.9. HSE mobile phone devices may not be used:

- For excessive personal use; Any usage over and above incidental usage is to be reimbursed to the HSE. Reimbursement should be made through the normal receipting channels. A €15 receipting threshold shall be applied i.e. where the amount owed is less than €15 the user must wait until the €15 is accumulated prior to reimbursement.
- 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 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 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 entering competitions either through premium rate text or on personal competition entry forms as this may give rise to the end user automatically subscribing the number to receive offers from that eternal company running the competition.
- 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.

27.10.10. The standard restrictions incorporated into the usage of mobile phone devices are as follows:

- 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 DG.

- The use of a mobile phone device to make calls while abroad is prohibited except in exceptional circumstances such as outlined in (a) to (d) above.

- HSE mobile phone devices must <u>not</u> be used to dial premium rate numbers (i.e. calls to telephone numbers beginning with the 15xx prefix – i.e. 1550, 1590 etc). HSE Mobile phone devices must not be used to text premium rate numbers and must not be used to subscribe to non work related services. Premium Rate texts numbers in general but not exclusively are five digit numbers beginning with 5 and are primarily ring tones subscriptions or competition lines.

- Internet Access
  Not granted or restricted to specific public/health specific sites.[3]

27.11. Security

27.11.1. 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/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/)'

27.11.2. 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 if reasonable precautions are not taken.

27.11.3. All use, management and security of confidential and personal information on a HSE mobile phone device is governed by the terms of the HSE Information Technology Acceptable Usage Policy - (http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/).

27.11.4. All storage of confidential and personal information on a HSE mobile phone device is governed by the terms of the HSE Encryption Policy - (http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/).

27.12. Confidentiality & Privacy

27.12.1. 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.

27.12.2. 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.

27.12.3. 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.

[3] *[3]Community Type Service Managers may have a requirement, driven by clinical / therapeutic or other needs, to make purchases on the internet. Such services will require written sanction from Assistant National Director of Service/equivalent salary Grade and or officer designate for departures from this procedure.*

27.13. Lost or stolen mobile phone devices

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

27.13.2. Local mobile phone device administrators must report the incident to their senior manager, the mobile phone service provider,

27.13.3. The Line Manager should notify the local Garda Siochana of the incident. Line Manager should also contact AFS & Governance Director re the insurance implication of the incident.

27.13.4. 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/).

27.14. Employees Leaving the HSE / Employee Transfers

27.14.1. Employees must return their HSE mobile phone device and any associated equipment (e.g. car kit, battery charger etc) to their line manager and local mobile phone device administrator when they leave the employment of the HSE. The local mobile phone administrator should contact ICT who shall immediately contact the relevant service provider to cancel the contract.

27.14.2. Employees transferring internally within the HSE must ensure that they notify the local mobile phone device administrators in the area they are leaving an area to ensure amendments are made to the register of mobile phone devices in particular to ensure the change in billing address where appropriate.

27.14.3. Employees who are retiring / resigning may, by agreement, purchase their mobile phone device 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 will be advised by the relevant Assistant National Director of ICT or his/her nominee.

27.15. Disposal of Mobile Phone Devices

27.15.1. Prior to disposal of a mobile phone device steps should be taken to ensure that all data on the device (e.g. contact numbers) is removed. Contact local ICT Division for assistance.

27.15.2. Old and obsolete HSE mobile phone devices must be recycled in accordance with the requirements of the Waste Electrical and Electronic Equipment (WEEE) directive. WEEE Ireland : The Irish Compliance Scheme for Electrical and Battery Recycling

27.16. Roles & Responsibilities

27.16.1. Line Managers

Line Managers (or their nominee) are responsible for:

- The implementation of this policy and all other relevant policies within their area of responsibility;

- Ensuring HSE mobile phone devices are only assigned to employees that satisfy the approved criteria ;

- Ensuring that all employees who hold HSE mobile phone devices within their area of responsibility are notified of the name and contact details of the local mobile phone device administrator.

- Ensuring that all mobile phone device costs incurred within their area of responsibility are:
  a) Necessary for the service;
  b) Represent value for money;
  c) Are appropriately monitored and controlled;
  d) Are reasonable in line with the employees duties:

- Implementing procedures within their own area of responsibility to ensure that excessive personal calls costs are reimbursed to the HSE;

- Put procedures in place to ensure all mobile phone devices and associated equipment (e.g. car kit, battery charger etc) are returned in a timely manner when an employee leaves the employment of the HSE or transfers to another HSE directorate or service area;

- Ensuring that processes are in place between mobile device users and the service provider to provide the regular suite of reports to facilitate review and monitoring of employees mobile phone device spend.

- Ensuring an up to date list of all mobile phone devices and associated equipment (e.g. car kit, battery charger etc) is held and maintained within their local office of area; The list must include the following information for each mobile phone device:

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

27.16.2. Local Mobile Phone Device Administrators:

Each local mobile phone device administrator is responsible for:

- Dealing with all administrative matters relating to the use of mobile phone devices within their local office e.g. invoice queries;
- Ensuring all completed and approved forms for new mobile phone devices, upgrades, replacements and account terminations are forwarded to their local ICT department in a timely manner;
- Ensuring that employees receive a copy of this policy and sign a copy of the HSE Mobile Phone Device User Agreement (Appendix B) 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;
- Liaise with Regional Mobile Phone Device administrator on issues relating to Mobile Phone Devices.

27.16.3. Regional Mobile Administrator

- Lead person within their region on all issues on Mobile Phone Devices.
- Coordinates the work of the Local Mobile Administrators in relation to their work on Mobile Phone Devices.
- Ensure compliance with National Mobile policies within their region.
- Liaises with the National ICT Lead, Mobile Phone Devices to ensure implementation of the award of the National Mobile Framework.

27.16.4. National ICT Lead, Mobile Phone Devices

- Ensuring adequate procedures are in place for approving and renewing the assignment of mobile phone devices for HSE employees.
- Leads the project working with Mobile Phone Service Providers, Regional Mobile Administrators, Procurement and Finance Department staff on the implementation of the award of the National Mobile Framework and on the adherence to HSE mobile policies/ mobile financial regulations.

27.16.5. ICT Directorate

The ICT Directorate is responsible for:

- Managing and logging the procurement of mobile phone devices on behalf of the HSE. This may include the following - ·

  New connections
  Upgrade phones/ devices
  Cancel accounts
  Remove roaming bar
  Remove international call bar
  Remove directory enquiry bar

- Holding the registers of contact details of all local mobile phone device administrators in their designated area.

- The management and monitoring of the centralised processing of mobile phone device bills and the distribution of summary reports to relevant Line Managers

27.16.6. *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;

- 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;

- Ensuring all excessive personal call costs are reimbursed to the HSE;

- 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;

27.16.7. *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.

27.17. Monitoring

27.17.1. 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.

27.17.2. 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.

27.17.3. 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.

27.17.4. Individual Line Managers must implement local procedures to monitor mobile phone usage within their directorate or service to ensure compliance with this policy.

27.18. Processing of Mobile phone device Bills

27.18.1. Reports shall be generated by mobile carriers and distributed within HSE for ongoing review and monitoring.

27.18.2. ICT need to ensure on a regular basis that service provider invoice values are audited by exception and benchmarked against average monthly expenditure.

27.18.3. Monthly spend per region shall be notified to each Regional Mobile Administrator and any large scale discrepancies are flagged and explanations sought from device user where required.

27.18.4. All mobile phone device invoices must be charged to the designated central ICT cost centre.

27.18.5. Any changes should be notified (i.e. employee leaving) immediately to Regional Mobile Device Administration section.

27.19. Health and Safety

27.19.1. 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 HSE will not be held liable for any breaches of this legislation.

27.19.2. The use of hands-free phone kits or Bluetooth technology is not an offence under the Act. The HSE is not obliged to provide Bluetooth or hands free car kits to an employee.

27.19.3. 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.

27.20. Segregation of Duties

27.20.1. It is the responsibility of each Integrated Service Area (ISA) Manager or equivalent grade or officers designate to ensure appropriate segregation of duties to eliminate possibility of collaboration.

27.21. Reporting of Irregularities

27.21.1. Any member of staff who considers that there may have been an irregularity that could lead to misappropriation of funds or an instance of fraud must communicate the facts surrounding this instance in writing to their Line Manager immediately. The Line Manager to whom the matter has been reported must inform their ISA Manager or equivalent, the Assistant National Director of Finance, the HSE National Director of Audit and HR for appropriate action. For further information please refer to HSE Policies, Procedures Guidelines and in particular to the HSE Protected Disclosures of Information Policy at HSENet - HSE National Intranet - Policies, Procedures & Guidelines

27.22. Audit

27.22.1. The external and internal auditors of the HSE have the right to unrestricted access to all premises, vouchers, documents, books of account, and computer data and to any other information which they consider relevant to their enquiries and which is necessary to fulfil their responsibilities. Both internal and external auditors also have the right to verify assets and the right of direct access to any employee or person responsible for the administration or management of HSE funds with whom it is felt necessary to raise and discuss such matters.

27.22.2. Sample checks by auditors may take place at regular intervals in each financial year.

27.22.3. Every officer shall attend at such place and at such time as may be appointed by the Auditor and shall submit his/her records, books and accounts for examination and checking.

27.22.4. Where any irregularities are disclosed at the checking of the accounts of an officer, the internal/external Auditor shall report such irregularities to the Chief Financial Officer, who shall cause a full investigation to be made and shall take all necessary action.