Document Control

Policy Title	Mobile Devices Policy
Policy Number	098
Owner	Information & Communication Technology Manager
Contributors	Information & Communication Technology Team
Version	1.0
Date of Production	01 October 2014
Review date	01 October 2016
Post holder responsible for review	Information & Communication Technology Manager
Primary Circulation List	Shared Drive
Web address	n/a
Restrictions	None

Version Control

Version Number	Owner	Description	Circulation
1.0	Information & Communication Technology Manager	Review	SMT

1.0 POLICY:

Sunbeam House Services (SHS) issues mobile devices to certain staffs that, as part of their role, need to access the organisation network from different locations.

SHS 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 devices could expose SHS 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 devices within SHS.

This policy is mandatory and by using any mobile devices which are owned or leased by SHS, users are agreeing to abide by the terms of this policy.

2.0 SCOPE:

This policy represents SHS's position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

- All mobile devices which are owned or leased by SHS and, users, holders and uses of such mobile phone devices.
- All SHS ICT resources which include equipment, systems and applications including cloud based applications.
- All users, and uses of SHS ICT resources;
- All connections to (locally or remotely) SHS network (Local Area Network (LAN)/Wide area network (WAN))

3.0 ROLES & RESPONSIBILITIES:

3.1 Users

Each user of SHS's ICT resources is responsible for:-

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

3.1.2 Respecting and protecting the privacy and confidentiality of the information they process at all times.

3.1.3 Complying with instructions issued by the ICT Manager on behalf of SHS.

3.1.4 Reporting all misuse and breaches of this policy to their Senior Manager.

3.2 Senior Managers

In addition to each user's responsibilites, Senior Managers are directly responsible for:-

3.2.1 The implementation of this policy and all other relevant SHS policies within the business areas for which they are responsible.

3.2.2 Ensuring that all SHS employees who report to them are made aware of and are instructed to comply with this policy and all other relevant SHS policies.

3.2.3 Consulting with the ICT Manager in relation to the appropriate procedures to follow when a breach of this policy has occurred.

3.3 ICT System Administrators & Developers

Each SHS System Administrator & Developer is responsible for:-

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

3.3.2 Complying with instructions issued by the ICT Manager on behalf of SHS.

4.0 GUIDELINES:

4.1 All SHS mobile devices and associated equipment (e.g. car kit, battery charger etc) must be purchased via the ICT Manager. The mobile devices, associated equipment and mobile accounts remain the property of SHS.

4.2 If a staff member needs to have SHS related personal information held on a mobile device and there is no other option, then they must contact the ICT Manager who will arrange to have the mobile device encrypted.

4.3 Each mobile device is authorised for use by a specific named individual or service. The responsibility for the physical safeguarding of the device will then rest with that named individual or staff team.

4.4 Mobile device billing

4.4.1 Users must identify and quantify all personal call charges and costs on the invoice and, return this along to the Account's office for payment processing

4.4.2 All personal charges outside of the fixed SHS tariff must be paid for by the user.

4.5 Lost or Stolen Mobile Devices

4.5.1 Users must report all lost or stolen mobile devices to 02 on 1909 and have their phone account suspended.

4.5.2 Users must notify their Senior Manager and ICT department to advise them.

4.5.3 Incidents where a lost or stolen SHS mobile device contains confidential or personal information must be reported by the user to the ICT Manger, Data

Protection Officer and Senior Services Manager without delay in line with the Data Breach Management Policy.

4.6 Usage

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

4.6.2 Mobile devices may only be used by an assigned SHS employee and must not be used by any other SHS employees or third parties without the prior authorization of the local Client Services Manager. Any usage made on an individuals SHS mobile device remains the responsibility of the assigned individual

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

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

4.7 Restrictions on Usage

4.7.1 Calls made from a SHS mobile 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 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:

4.7.1.1 A user is out of the country on official SHS business.

4.7.1.2 A user is working off-site or out of hours and needs to contact an external service provider / consultant based abroad.

4.7.1.3 In case of an emergency.

4.7.1.4 Or at the discretion of the relevant Senior Services Manager or the Managing Director.

4.7.2 SHS mobile 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).

4.8 Employees Leaving SHS / Employee Transfers

4.8.1 Employees must return their SHS mobile device and any associated equipment (e.g. car kit, battery charger etc) to the local Client Services Manager before they leave the employment of SHS.

4.8.2 Employees transferring internally within SHS must ensure that they notify the ICT Manager.

4.8.3 Employees who are retiring / resigning may, by agreement, purchase their mobile phone and if they wish have the account transferred to their name.

4.9 Confidentiality

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

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

4.9.3 Mobile devices equipped with cameras must not be used inappropriately within SHS. In this regard users must not:

4.9.3.1 Take photographs or video recordings using a SHS mobile device or any other device in areas where an employee or client has a reasonable expectation of privacy.

4.9.3.2 Distribute photographs, videos or recordings of any type using SHS mobile devices within SHS, unless the content and use is for SHS purpose's.

4.10 Security

4.10.1 Users must ensure their SHS mobile device is protected at all times. At a minimum all mobile devices must be protected by the use of a Personal Identification Number (PIN). Users must not disable this PIN request on basic mobile phone device. Smartphones and tablets must also have a passcode and time out set.

4.10.2 All mobile devices should be password/passcode-protected to prevent unauthorised use of the device and unauthorised access to information held on the device as per SHS's *Password Standards Policy*.

4.10.3 Users must take all reasonable steps to prevent damage or loss to their mobile device. The user may be responsible for any loss or damage if reasonable precautions are not taken.

4.10.4 All use, management and security of confidential and personal information on a SHS mobile device is governed by the terms of SHS's *Information Technology Acceptable Usage Policy.*

4.11 Email & Internet

4.11.1 Where a mobile device is capable of allowing email and/or internet access, all use of these facilities on the mobile device is governed by the terms of SHS's *Electronic Communications Policy*.

4.12 Health & Safety

4.12.1 For legal reasons and in the interest of public and personal safety, the use of SHS mobile 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.

4.13 Software and Electronic Media

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

4.13.2 Mobile devices must not contain unlicensed software. Personally licensed software that will impede or damage SHS's resources must not be installed.

4.13.3 Only software which has the correct and proper license and has been purchased and/or approved by the ICT Manager may be installed and used within SHS.

4.13.4 All software and electronic media developed and purchased on behalf of SHS remains the property of SHS and must not be used, copied, distributed or borrowed without the authorisation of SHS.

4.13.5 The ICT Manager on behalf of SHS reserves the right to remove software at any time, for reasons including but not limited to:-

4.13.5.1 non-compliance with SHS policies,

4.13.5.2 the software is not properly licensed, or

4.13.5.3 the software is found to have a negative impact on the performance of SHS network, systems or equipment.

4.14 Information Disposal

4.14.1 Confidential and personal information must be securely deleted when it is no longer required in line with Data Protection. All traces of the information must be removed from mobile devices before they are reused within SHS, sold to employees, donated to charity, or recycled. The simple deletion or formatting of information is not sufficient to remove all traces of the information. The information must be overwritten using special sanitation software which is available from the ICT Manager or the mobile device used to store the information must be physically destroyed.

4.15 Disposal of Mobile Devices

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

4.16 Virus and Malicious Software Protection

4.16.1 Mobile devices which are not regularly connected to the network may not have their anti-virus/spyware software updated automatically.

4.16.2 All ICT resources that do not connect regularly to the network should have a standalone version of anti-virus.

4.16.3 Users who receive a virus warning message must notify the ICT Department. Under no circumstances should they forward it on to other users.

4.17 Monitoring

4.17.1 SHS reserves the right to record, examine and maintain logs of any, or all uses of its ICT resources, in order to:

4.17.1.1 Help trace and resolve technical faults.
4.17.1.2 Protect and maintain network and system security.
4.17.1.3 Maintain system performance and availability.
4.17.1.4 Ensure the privacy and integrity of information stored on SHS network.
4.17.1.5 Investigate actual and suspected security incidents.
4.17.1.6 Prevent, detect or minimize inappropriate use.
4.17.1.7 Protect the rights and property of SHS, its employees and clients.
4.17.1.8 Ensure compliance with SHS policies, current legislation and applicable regulations.

4.17.2 While SHS does not routinely monitor an individual user's use of its ICT resources, 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 individual login sessions, contents of hard disks, internet sites visited, telephone usage and the content of electronic communications.

4.17.3 The monitoring of an individual user's ICT activity must be authorised by the Managing Director and the individual's Senior Services Manager. The results of all monitoring will be stored securely and will only be shared with those authorised to have access to such information.

4.18 Unacceptable Use

SHS ICT resources may not be used for:-

4.18.1 For excessive personal use
4.18.2 For personal commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
4.18.3 For political activities, such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions;
4.18.4 To knowingly misrepresent SHS;
4.18.5 To transfer unencrypted confidential or personal information onto any mobile storage device or resource, i.e. (drop box, icloud), etc.
4.18.6 To enter into contractual agreements inappropriately (i.e. without authorisation or where another form of agreement is required);
4.18.7 To view, create, download, host or transmit (other than for properly authorised and lawful purposes) pornographic, offensive or obscene material (i.e. information, images, video clips, audio recordings etc.), which could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs;
4.18.8 To retrieve, create, host or transmit material which is designed to cause annoyance, inconvenience or needless anxiety to others;
4.18.9 To retrieve, create, host or transmit material which is defamatory;

4.18.10 For any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);

4.18.11 For any activity that would compromise the privacy of others;

4.18.12 For any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to SHS or others;

4.18.13 For any activity that would intentionally waste SHS's resources (e.g. employee time and ICT resources);

4.18.14 For any activity that would intentionally compromise the security of SHS's ICT resources, including the confidentiality and integrity of information and availability of ICT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection);

4.18.15 For the unauthorised installation and use of software or hardware tools which could be used to probe or break SHS ICT security controls;

4.18.16 For the installation and use of software or hardware tools which could be used for the unauthorised monitoring or interception of electronic communications within SHS or elsewhere;

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

4.18.18 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 SHS's ICT resources may exist.

5.0 ENFORCEMENT

5.1 SHS reserves the right to take such action as it deems appropirate against users who breach the guidelines of the policy

5.2 Breaches of this policy by a third party, may lead to the withdrawal of SHS information technology resources to that third party and/or the cancelleation of any contract(s) between SHS and the third party.

5.3 SHS will refer any user of its ICT resources for illegal activities to the appropriate law enforcement agencies.