Document Control

Policy Title	Information Technology Acceptable Usage Policy
Policy Number	095
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) is committed to the correct and proper use of its Information Communication Technology (ICT) resources in support of its administrative and service functions.

The inappropriate use of ICT resources could expose SHS to risks including, virus attacks, theft and disclosure of information, disruption of network systems and services or litigation. The purpose of this policy is to define acceptable use of ICT resources within SHS.

This policy is mandatory and by accessing any ICT resources 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 SHS ICT resources which include equipment, systems and applications including cloud based applications.
- All users, holders and uses of SHS ICT resources;
- All connections to (locally or remotely) SHS network (Local Area Network (LAN)/Wide area network (WAN))
- All connections made to external networks through SHS network and using SHS equipment/devices.

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 When prompted to change their password either by ICT Member of staff or by SHS computer system to change it to do so as soon as possible.

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

3.1.5 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 themare 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 Ensuring the network administration password is secure.
3.3.3 Complying with instructions issued by the ICT Manager on behalf of SHS.

3.4 Systems Developers

In addtion to the above responsiblities all system developers (including third party contractors) who are responsible for developing systems for SHS, must ensure that their systems contain the following security features:-

3.4.1 They must support authentication of individusers and not just groups.
3.4.2 They must not store passwords in clear text or in any easily reversible form
3.4.3 They must provide for some sort of role management, such that one user cannot take control of the functions of another without having a knowledge of the other users passwords.

4.0 POLICY:

4.1 Principles of Acceptable Use

The acceptable use of SHS ICT Resources is based on the following principles:

4.1.1 SHS's ICT resources are to be used primarily for SHS work-related purposes. Occasional personal use maybe permitted provided that this does not incur any significant costs to SHS, or interfere with the performance, work, duties, and responsibilities of the user and SHS.

4.1.2 Users must ensure that they use ICT resources at all times in a manner which is lawful, ethical and efficient.

4.1.3 Users must respect the rights and property of others, including privacy, confidentiality and intellectual property.

4.1.4 Users must respect the integrity and security of the SHS's ICT resources.

4.2 Monitoring

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

4.2.1.1 Help trace and resolve technical faults.

4.2.1.2 Protect and maintain network and system security.

4.2.1.3 Maintain system performance and availability.

4.2.1.4 Ensure the privacy and integrity of information stored on SHS network.

4.2.1.5 Investigate actual and suspected security incidents.

4.2.1.6 Prevent, detect or minimize inappropriate use.

4.2.1.7 Protect the rights and property of SHS, its employees and clients.

4.2.1.8 Ensure compliance with SHS policies, current legislation and applicable regulations.

4.2.2 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.

4.2.3 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.

4.3 Network Accounts & Passwords

4.3.1 Where technically possible all SHS Information Technology (ICT) equipment, systems and applications must be protected by the use of strong passwords.

4.3.2 All passwords must meet the requirements of the Password Standards Policy

4.3.3 ICT System Administrators and Developers must ensure each user is assigned a unique account name and password set which will enable them to access the appropriate SHS ICT resources.

4.3.4 In exceptional circumstances, the ICT Manager will approve group accounts.

4.3.5 Users must only use accounts and passwords which have been assigned to them.

4.3.6 Users must ensure all account and passwords assigned to them are kept confidential at all times, are not shared with others, or written down anywhere that can be access by others.

4.3.7 Each user is responsible for all activities performed on any SHS device or system while logged in under their account and password.

4.3.8 Users must change their passwords at least every 90 days on any SHS device that they have or when instructed by an ICT staff member.

4.4 Software and Electronic Media

4.4.1 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.

4.4.2 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.

4.4.3 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.

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

4.4.4.1 non-compliance with SHS policies,

4.4.4.2 the software is not properly licensed,

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

4.5 Purchase of ICT Equipment

4.5.1 All ICT equipment should be purchased through the ICT Manager using the ICT Resource Request Form.

4.5.2 Users must not:-

4.5.2.1 Connect or disconnect any ICT equipment to or from SHS network without the prior authorisation of the ICT Manager.

4.5.2.2 Connect any SHS ICT equipment to an external network without the prior authorisation of the ICT Manager.

4.5.2.3 Connect any device to their local computer without the prior authorisation of the ICT Manager.

4.5.2.4 Alter the hardware or software configuration of ICT equipment without the prior authorisation of the ICT Manager.

4.5.3 ICT equipment must be physically secured and positioned in such a way as to minimise the risk of unauthorised individuals accessing the equipment or viewing information displayed on the screen. Users must ensure that they

either log off or 'lock' their device when they have to leave it unattended for any period of time.

4.5.4 All ICT equipment provided by SHS remains the property of SHS. Users must not remove or borrow ICT equipment without the authorisation of their Senior Services Manager. The security of any equipment borrowed is the responsibility of the borrower and the equipment must be returned by the borrower before they leave the employment of SHS or, at the request of the borrower's Senior Services Manager or the ICT Manager.

4.5.5 Old and obsolete ICT equipment must be recycled in accordance with the requirements of the *Electrical and Electronic Equipment (WEEE) Directive*. Users must notify the ICT Manager of old equipment and they will facilitate the collection and disposal of the equipment.

4.5.6 Users must take due care when using ICT equipment and take reasonable steps to ensure that no damage is caused to the equipment. They must not use ICT equipment if they have reason to believe it is dangerous to themselves or others.

4.5.7 Users must report all damaged, lost or stolen ICT equipment to their Senior Services Manager and the ICT Manager. Incidents where lost or stolen ICT equipment contains confidential or personal information must be reported to the ICT Manager, Data Protection Officer and relevant Senior Services Manager immediately.

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

4.5.8.1 non-compliance with SHS policies;

4.5.8.2 the equipment does not meet approved specification and standard

4.5.8.3 the equipment is deemed to be interfering with the operation of the network.

4.6 Telephone System

4.6.1 Access to SHS telephone system is primarily intended for SHS work related purposes. The making and taking of personal calls is not strictly prohibited, however users must keep this to a minimum.

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

4.6.3 The use of SHS mobile phone devices is governed by the requirements of SHS *Mobile Device Policy*.

4.6.4 The use of SHS facsimile (fax) machines is governed by the requirements of SHS *Electronic Communications Policy*.

4.7 Electronic Communications

4.7.1 All email use within SHS is governed by requirements of SHS *Electronic Communications Policy.*

4.8 Internet

4.8.1 All internet use within SHS is governed by requirements of SHS *Electronic Communications Policy.*

4.9 Social Media

4.9.1 All social media use within SHS is governed by requirements of SHS *Social Media Policy.*

4.10 Confidentiality and Privacy

4.10.1 Users must respect the privacy and confidentiality of information at all times and must not access information unless they have a valid work-related reason or have been granted permission.

4.10.2 Information must not be copied, renamed, deleted or modified without authorisation. This includes information on storage devices and information in transit.

4.10.3 Confidential and personal information must only be discussed or shared with other SHS employees and third parties who have a valid work-related reason and are authorised to have access to the information.

4.10.4 In circumstances where a user is on-leave or out of the office their Senior Services Manager may be permitted to access their computer system to retrieve documents or emails necessary to deal with routine work-related matters. The procedure for this is that ICT will reset all network passwords.

4.11 Information Storage

4.11.1 Where possible all confidential and personal information must be stored on a secure SHS network server with restricted access. In circumstances where it has been deemed necessary to store such information on any device other than a SHS network server, the information must be encrypted.

4.11.2 The storage of confidential or personal information on USB flash drives is strictly prohibited unless it is a device that has been provided by ICT and is encrypted.

4.11.3 The storage of confidential and personal information on any device which is not owned or leased by SHS is prohibited without the prior authorisation of the relevant information owner and ICT Manager.

4.11.4 SHS Network servers are reserved for the storage of SHS work-related information only.

4.12 Information Backup

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

4.13 Information Security

4.13.1 In accordance with the provisions of the *Data Protection Act 1988 and 2003*, users who are responsible for storing personal information must ensure that the privacy and security of the information is not compromised.

4.13.2 Users must report all actual or suspected breaches of information confidentiality and security to the ICT Manager, Data Protection Officer and to the relevant Senior Services Manager immediately.

4.14 Information Transfer

4.14.1 All transfer of confidential and personal information to third parties must be authorised by the individual concerned and/or Managing Director.

4.14.2 Where information is disclosed for testing or research purposes, it must where possible be anonymised.

4.14.3 Only the minimum amount of information must be transferred as is necessary for a given task to be carried out,

4.14.4 Where possible all transfer(s) of confidential and personal information must be carried out electronically in line with the requirements of SHS *Electronic Communications Policy*.

4.15 Information Disposal

4.15.1 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 old computers, mobile devices and removable storage 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 computer device used to store the information must be physically destroyed.

4.16 Virus and Malicious Software Protection

4.16.1 SHS desktop and laptop computers which are regularly connected to SHS network will have their anti-virus/spyware software updated automatically. Computers 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 Unacceptable Use

SHS ICT resources may not be used for:-

4.17.1 For excessive personal use;

4.17.2 For personal commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;

4.17.3 For political activities, such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions;

4.17.4 To knowingly misrepresent SHS;

4.17.5 To transfer confidential or personal information onto any unencrypted mobile storage device or resource;

4.17.6 To enter into contractual agreements inappropriately (i.e. without authorisation or where another form of agreement is required);

4.17.7 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;

4.17.8 To retrieve, create, host or transmit material which is designed to cause annoyance, inconvenience or needless anxiety to others;

4.17.9 To retrieve, create, host or transmit material which is defamatory;

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

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

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

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

4.17.14 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);

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

4.17.16 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;

4.17.17 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;

4.17.18 For any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law;

4.17.19 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.