Document Control

Policy Title	Remote Working Policy
Policy Number	102
Owner	Information & Communication Technology Manager
Contributors	Information & Communication Technology Team
Version	1.0
Date of Production	28 April 2015
Review date	28 April 2017
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	New	SMT

1.0 POLICY:

Remote working is a work arrangement in which employees do not commute to a central place of work. Many remote workers work from home, while others, sometimes called 'nomad workers' use mobile telecommunications technology to work from other locations.

Remote working must only be undertaken with the permission of the Information & Communication Technology (ICT) Manager, subject to authorisation by the individual's Senior Services Manager (SSM).

2.0 SCOPE:

This policy is not intended to create an obstacle to remote working, and nor is intended to support or advocate working from home. Its purpose is to provide controls in respect of remote access to Sunbeam House Services (SHS)'s information assets to protect both individuals and SHS from the consequences of accidental disclosure or loss of such information.

This Policy is primarily directed at:

- those who access SHS's systems from home or other remote locations using either privately owned, third-party-owned or SHS owned equipment; and,
- ICT Staff who are responsible for systems that are accessed by users remotely.

Relevant requirements naturally extend to anyone else who is subjected to the Policy framework who undertakes activities governed by this Policy.

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 Information Technology (ICT) resources which include equipment, systems and applications including cloud based applications.
- All users, and uses of SHS Information Technology (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 policies apply when working remotely

4.2 User's must take cognisance of security issues when working remotely.

4.3 Confidentiality and Privacy

4.3.1 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 and have been granted permission.

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

4.3.3 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.

4.3.4 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.

4.4 Information Storage

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

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

4.4.3 The storage of confidential and sensitive 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.

4.4.4 SHS storage resource are reserved for the storage of SHS work-related information only.

4.4.5 As present legislation exists please note the difference between personal and sensitive personal data exists in the legislation.

4.5 Information Backup

4.5.1 Users who do not have access to a SHS storage resource 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.

4.6 Information Security

4.6.1 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.

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

4.7 Information Transfer

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

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

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

4.7.4 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.

4.8 Information Disposal

4.8.1 In the context of the remote working policy the information disposal has a particular context such as old computers. 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. All SHS information is removed from redundant equipment with assistance from the ICT Department.

4.9 Virus and Malicious Software Protection

4.9.1 Remote workers must ensure that the resource they are using has up-to-date anti-virus/spyware software before remote access to SHS resources is undertaken.

4.9.2 Where it is suspected that an IT device has been infected with virus and/or maliciious software, no access must be undertaken to SHS resources.

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

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.