Document Control

Policy Title	Encryption Policy
Policy Number	092
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:

The purpose of this policy is to define the acceptable use and management of encryption software and hardware throughout Sunbeam House Services (SHS).

This policy is mandatory and by accessing any Information Technology (ICT) resources which are owned or leased by SHS, users are agreeing to abide by the terms of this policy.

Encryption is the process of encoding information in such a way that eavesdroppers or hackers cannot read it, but authorized parties can.

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, 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 polciies, 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 Ensuring the network administration password is secure.

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

4.0 GUIDELINES:

4.1 Where possible all confidential and personal information must be stored on a secure Sunbeam House Services network server with restricted access. Where it has been deemed necessary by the information owner to store confidential or personal information on any device other than a SHS network server the information must be encrypted.

4.2 All passwords used as part of the process to encrypt/decrypt information must meet the requirements of SHS's Password Standards Policy

4.3 All SHS mobile devices must have SHS approved encryption software installed prior to their use within SHS. In addition to encryption software the laptop must be password protected and have up-to-date anti-virus software installed.

4.4 The preferred method of encryption for laptop computers and other mobile computer devices is whole disk encryption. Mobile computer devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all confidential and personal information stored on the device.

4.5 Laptop and mobile computer devices must not be used for the long-term storage of confidential information.

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.