Document Control

Policy Title	Electronic Media Disposal Policy
Policy Number	091
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:

Data is being transmitted and stored on computer systems and electronic media by virtually every person conducting business for Sunbeam House Services (SHS). Some of that data contains sensitive information, including client records, personnel records, financial data, and protected health information. If the information on those systems is not properly removed before the equipment is disposed of, or transferred within SHS, that information could be accessed and viewed by unauthorized individuals. As such, all users of computer systems within SHS, including contractors and vendors with access to SHS systems, are responsible for taking the appropriate steps, as outlined below to ensure that all computers and electronic media are properly sanitized before disposal.

Electronic Media is defined as any electronic storage device that is used to record information, including, but not limited to hard disks, magnetic tapes, compact disks and digital video disks.

A wide variety of information resources contain electronic media including, but not limited to:

- computer systems, personal desktop assistants, smart phones, removable storage devices
- such as USB storage devices, copy machines and fax machines.

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 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 instructions issued by the ICT Manager on behalf of SHS.

4.0 GUIDELINES:

4.1 Initiation

All electronic media must be properly sanitized before it is transferred from the custody of its current owner. The proper sanitization method depends on the type of media and the intended disposition of the media.

4.1.1 **Overwriting Media for Sanitization**: Overwriting is an approved method for sanitization storage media. Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented. SHS encourages use of certified sanitization software such as available through the ICT Manager
4.1.2 **Destruction of Media**: Destruction is the process of physically damaging a medium so that it is not usable by any device that may normally be used to read electronic information on the medium, such as a computer, personal hand held device, audio or video player. SHS encourages that destroyed media, such as hard drives, be processed through Waste Electical when appropriate.

All data governed by a data retention policy must be processed appropriately before the media on which it is stored is disposed of.

4.2 Disposal of Hard Drives

4.2.1 **Transfer and disposal of hard drives to other sections or outside of SHS**: Prior to transfer, operable hard drives must be overwritten. Degaussing is not an effective means of data destruction on hard drives. Equipment designated for surplus or other disposal should have a label affixed stating that the hard drive has been properly sanitized.

4.2.2 **Transfer of hard drives within a department:** Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. All hard drives should be sanitized, however; since the drive is remaining within the section, the hard drive may instead be formatted prior to transfer

4.2.3 **Sending a hard drive out for repair, return or for data recovery:** The vendor repairing or recovering data on the hard drive must sign an appropriate agreement with SHS, insuring that the vendor will take proper care of the data. When possible, the vendor should return the defective media for proper disposal as described in this standard.

4.2.4 **Disposal of damaged or inoperable hard drives:** The owner must first attempt to overwrite the storage device. If the device can not be overwritten, the device must be disassembled and mechanically damaged so that it is not usable by a computer.

4.3 Disposal of electronic media other than hard drives

4.3.1 **Transfer and disposal to other departments or outside of SHS**: All electronic media must be erased, degaussed, or rendered unusable before leaving the custody if its current user.

4.3.2 **Transfer within a department**: Before electronic media is transferred from the custody of the current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media should be erased if the media type allows it or destroyed if erasure is not possible.

4.4 Violation of Standard

If there is a reasonable basis to believe that the proper procedures as outlined in this standard have not been or are not being followed, a report must be filed with the ICT Manager. If improperly sanitized electronic media is found, then the media should be reported to ICT support personnel.

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.