Document Control

Policy Title	ICT Backup Policy
Policy Number	093
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 Manager	Review	SMT

1.0 POLICY:

This policy defines the information backup service within Sunbeam House Services (SHS).

It is the responsibility of the user to back up information stored locally on devices. Please adhere to policy when storing information locally.

This policy is designed to protect systems and data in SHS to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

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 Users that need files restored must submit a request to the help desk, including information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed. Files will be restored to their original location only.

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 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 On receiving instruction from user to restore the relevant information to its previous location.

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

3.3.3 The delegated ICT System Administrator & Developer shall develop a procedure for testing backups. The delegated ICT System Administrtor & Developer will test restore a sample of data on a monthly basis.

3.4 ICT Manager

3.4.1 ICT Manager will receive a notifcation of the status of the daily backup from the external backup company. Where the log indicates that a backup has failed the ICT Manager will notify the helpdesk to take appropriate action.

3.4.2 Where SHS data and where relevant the configuration is stored at a remote hosting location the ICT Manager will receive assurance from the host provider that backup of SHS data is undertaken.

3.4.3 The ICT Manager will ensure that systems are in place to backup SHS data and where appropriate systems configuration

4.0 GUIDELINES:

4.1 Definition

4.1.1 Backup is the saving of files onto offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

4.1.1.1 *Full backups* contain all the information needed to restore a service.

4.1.1.2 *Differential backups* contain the cumulative changes since the last full backup.

4.1.1.3 *Incremental backups* are similar to differential backups, except that they reflect only the changes since the previous differential backup; they don't compare with the original full backup directly.

4.1.2 Archive – the saving of older unused data onto offline mass storage media for the purpose of releasing on-line storage room

4.1.3 Restore – the process of bringing offline storage data back from the offline media and putting in on an online storage system such as a file server.

4.2 Timing

4.2.1 Backups are performed nightly on the servers to an off site data centre location.

4.2.2 Data is kept in two separate data centre locations.

4.3 External Hard Drive

4.3.1 Every 6 months SHS received a full backup of all the previous 6 months data on an encrypted external hard drive.

4.3.2 This hard drive is kept in the fire safe in SHS.

5.0 ENFORCEMENT

5.1 SHS reserves the right to take such action as it deems appropriate 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 cancellation 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.