Document Control

Policy Title	Data Management Policy
Policy Number	087
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 Data Management Policy is to protect the electronic data and information belonging to, or held by, Sunbeam House Services (SHS), by providing a framework within which the roles and responsibilities of those who manage or use the data and information are defined. The intention of the Policy is to enable access to data and information held by SHS, to the greatest extent possible, consistent with legislation and relevant SHS policies, whilst ensuring that data is protected from unauthorised use and breaches of privacy.

This Policy covers any information or data held by SHS that is stored electronically.

The Policy has been formulated on the basis of the following principles:

The data generated and/or held by SHS are key strategic assets that must be correctly managed and controlled so as to ensure their availability, integrity and confidentiality and to protect SHS's resources, reputation, legal position and ability to conduct its business.

SHS values the privacy of the individual and the management of data and information must be handled in way that protects that privacy.

The Policy is consistent with the terms of the following legislation:

- The Freedom of Information Acts, 1997 and 2003
- The Data Protection Acts, 1988 and 2003
- Copyright and Related Rights Act, 2000

The Policy should be read in conjunction with the following SHS policies:

- SHS Records Management Policy
- SHS Data Protection Policy
- SHS Electronic Communications Policy

The Policy will be reviewed regularly to ensure that it continues to reflect best practise in SHS.

2.0 DEFINITIONS:

2.1 DATA

"Data" means information in a form which can be processed and is a general term meaning facts, numbers, letters and symbols collected by various means and processed to produce information. Please note: this Policy only refers to **electronic** data (i.e. data held on computer or other electronic device).

2.2 PROCESSING

"Processing" means performing any operation or set of operations on data, including:

- Obtaining, recording or keeping data;
- Collecting, organising, storing, altering or adapting the data;
- Retrieving, consulting or using the data;
- Disclosing the information or data by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, erasing or destroying the data.

2.3 PERSONAL DATA

"Personal data" means data related to an individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into the possession of the Data Controller. Personal data would include the age of the individual, their home address, their educational and employment history, information relating to their financial affairs, marital status.

2.4 SENSITIVE PERSONAL DATA

"Sensitive personal data" means personal data relating to:

- The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject;
- Whether the data subject is a member of a trade-union;
- The physical or mental health or condition or sexual life of the data subject;
- The commission or alleged commission of any offence by the data subject; or
- Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

2.5 DATA CONTROLLER

"Data Controller" means the body which ultimately controls the content and use of data. Under this policy, the Data Controller means Sunbeam House Services. SHS, rather than any individual, location, administrative unit, ultimately owns all data held by SHS.

2.6 DATA OWNER

"Data Owner" means the most senior person in location/administrativeunit within which the data is created or stored unless this role has been explicitly and formally delegated to someone else by the most senior person in the aforementioned areas. Data owners have overall responsibility for the quality and integrity of the data held in their area. Further explanation of this term is provided below.

2.7 DATA CUSTODIAN

"Data Custodian" means an individual or location/administrative unit (e.g. ICT) to which data is entrusted on behalf of the Data Controller for the purposes of storage and/or processing.

2.8 DATA USER

"Data User" means any person who uses, processes, stores, manipulates data held by SHS.

2.9 DATA SUBJECT

A "data subject" means an individual who is the subject of personal data.

3.0 ROLES & RESPONSIBILITIES:

3.1 THE DATA OWNER

Every set of data has a Data Owner. The Data Owner has overall responsibility for the quality and integrity of the data. Specifically, the Data Owner is responsible for:

- deciding the criticality and sensitivity of the data;
- authorising access to and use of the data and regularly reviewing access privileges;
- assessing the risks to the data;
- ensuring that appropriate backup and contingency plans are developed for the data.

The Data Owner is the most senior person in the area within which the data is created or stored unless this role has been explicitly delegated to someone else. In the case of the data for the central systems in SHS, relating for example, to service users, personnel, or finance, the data owner will be designated by SHS. Where someone creates or uses a set or subset of data of which no one else may be aware, then that person assumes the relevant responsibilities of the data owner for that data.

Data owners must ensure that the SHS's Data Protection Policy is adhered to at all times.

An inventory will be maintained by the Data Protection Officer of all SHS's major electronic information assets and the ownership of each asset will be clearly stated. Within the information inventory, each information asset will be classified according to sensitivity and criticality.

3.2 THE DATA CUSTODIAN

In many cases data will be entrusted to an individual or a location/administrative unit (e.g. ICT) for the purposes of storage and/or processing in which case they take on the responsibilities of the Data Custodian. The Data Custodian is responsible for:

- maintaining the integrity and confidentiality of the data entrusted to them;
- ensuring that access to the data is restricted to those individuals authorised by the data owner;
- ensuring that all processes undertaken on the data have been authorised by the data owner;
- having adequate backup and recovery procedures in place for the data;
- providing any information necessary for the Data Owner to fulfil their responsibilities.

3.3 THE DATA USERS

Anyone using or processing SHS data must ensure that they do so in a manner that safeguards and protects the integrity, confidentiality and availability of the data at all times. They must comply with the relevant policies of SHS (as may be amended from time to time) and with all legal requirements, particularly in relation to data protection and copyright. The data should be used only for the purposes approved by the data owner.

Data Users should be especially vigilant in complying with this policy when transferring data to mobile equipment such as laptops, USB memory sticks, PDAs, DVDs, etc.

Anyone accessing information systems remotely to support the business activities of SHS must be authorised to do so by an appropriate authority within SHS. A risk assessment based on the criticality of the information asset being used must be carried out.

Removal off-site of sensitive data must be properly authorised by management. Prior to authorisation, a risk assessment based on the criticality of the information asset should be carried out.

Sensitive data or information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured throughout the transfer. Please refer to SHS's IT Security Policy and Guidelines on Encryption.

Unsolicited electronic mail should not receive serious attention until and unless the sender's identity and authenticity of the mail have been verified.

Prior to sending information or documents to third parties via email, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party must also continue to assure the confidentiality and integrity of the information. Email addresses should be checked carefully prior to dispatch.

Where the information is of a personal or sensitive nature, extra vigilance is required. Data Users should not send personal or sensitive information via email. Data Users are also required to comply with SHS's Data Protection Policy and the Data Protection Acts, 1988 and 2003, regarding disclosure of information outside of SHS.

Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

When permanently disposing of equipment containing storage media, all sensitive data and licensed software must be irretrievably deleted before the equipment is moved off site.

Any third party used for external disposal of the SHS's obsolete data-bearing equipment must be able to demonstrate compliance with the SHS's information security policies and also, where appropriate, enter into a service level agreement which documents the performance expected and the remedies available in case of non-compliance.

4.0 ENFORCEMENT

4.1 SHS reserves the right to take such action as it deems appropirate against users who breach the guidelines of the policy

4.2 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.

4.3 SHS will refer any user of its ICT resources for illegal activities to the appropriate law enforcement agencies.