Document Control

Policy Title	Data Breach Management Policy
Policy Number	086
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:

Sunbeam House Services (SHS) is obliged under Data Protection legislation to keep personal data safe and secure and to respond promptly and appropriately in the event of a personal data security breach. It is vital to take prompt action on foot of any such actual, potential or suspected security breach to avoid the risk of harm to individuals, damage to operational business and financial, legal and reputational costs to SHS.

The purpose of this policy is to provide a framework for reporting and managing security breaches involving personal or sensitive personal data. These guidelines may be used by all members of SHS in a combined effort to minimise the damage done by personal data security breaches.

This policy is mandatory and by accessing any of the SHS's Information/data, users are agreeing to abide by the terms of this policy.

2.0 WHAT IS A PERSONAL DATA SECURITY BREACH?

A personal data security breach is any incident which gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data held by SHS.

Personal data security breaches may occur in a variety of contexts, such as:

- Loss or theft of data, equipment on which data is stored (e.g. a memory stick) or paper records
- Inappropriate access controls allowing unauthorised use of information (e.g. uploading personal data to an unsecured web domain, using unsecure passwords)
- Equipment failure
- Confidential information left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account)
- Disclosing confidential data to unauthorised individuals
- Collection of personal data by unauthorised individuals
- Human error/accidental disclosure of data (e.g. emails containing personal or sensitive information sent to the wrong recipient)
- Hacking, viruses or other security attacks on IT equipment systems or networks
- Breaches of physical security (e.g. forcing of doors/windows/filing cabinets)

If there is any doubt as to whether a personal data security breach has occurred, the Data Protection Officer should be consulted immediately. This policy applies to all personal data created or received by SHS in any format, including data that is accesssed remotely.

Personal data is defined as information relating to a living individual who is or can be identifed from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of SHS.

3.0 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))

4.0 LEGISLATION

SHS has an obligation to abide by all relevant Irish legislation and European legislation. The relevant acts, which apply in Irish law to Information Systems, include but are not limited to:

- The Data Protection Act (1988/2003)
- European Communities Data Protection Regulations, (2001)
- European Communities (Data Protection and Privacy in Telecommunications) Regulations (2002)
- Data Protection EU Directive 95/46/EC
- Criminal Damages Act (1991)

5.0 PROCEDURE FOR REPORTING PERSONAL DATA SECURITY BREACHES

Any personal data security breach must be dealt with immediately and appropriately.

If a member of SHS becomes aware of an actual, potential or suspected breach of data security, he/she must report the incident to the Data Protection Officer immediately.

After reporting the incident, he/she must complete the Personal Data Security Breach Report form and email it to the Data Protection Officer as soon as possible.

6.0 PROCEDURE FOR MANAGING PERSONAL DATA SECURITY BREACHES

Upon receiving notification of a personal data security breach, the Data Protection Officer shall, in conjunction with any appropriate members of staff, take the following steps (in line with best practice) when responding to the breach.

6.1 Identification and initial assessment of the incident

If any member of SHS considers that any data security breach has, or might have, occurred, they must report this breach immediately to the Data Protection Officer and complete the Personal Data Security Breach Report form.

The Personal Data Security Breach Report form will assist the Data Protection Officer in conducting an initial assessment of the incident. This assessment will take into account:

- Whether a personal data security breach has taken place
- The nature of the personal data involved in the breach (i.e. whether sensitive personal data is involved)
- The cause of the breach
- The extent of the breach (i.e. the number of individuals affected)
- The potential harms to which affected individuals may be exposed
- Any steps that may be taken to contain the breach

Following this initial assessment of the incident, the Data Protection Officer may, according to the severity of the incident, consult with the Managing Director and decide if it is necessary to appoint a group of relevant SHS stakeholders (e.g. ICT, Human Resources) to assist with the investigation and containment process.

6.2 Containment and Recovery

In the event of a personal data security breach, immediate and appropriate steps must be taken to limit the extent of the breach.

The Data Protection Officer, in consultation with any relevant SHS staff, will:

- Establish who within SHS needs to be made aware of the breach (e.g. ICT, Human Resources) and inform them of their expected role in containing the breach (e.g. isolating a compromised section of the network)
- Establish whether there is anything that can be done to recover any losses and limit the damage caused by the breach
- Where appropriate, inform the Gardaí (e.g. in cases involving criminal activity)

6.3 Risk Assessment

The Data Protection Officer, in conjunction with any relevant SHS staff, will use the information provided in the Personal Data Security Breach Report form to fulfil the requirement to consider the potential adverse consequences for individuals, including how likely such adverse consequences are to materialise and how serious or substantial they are likely to be.

An assessment of the risks for SHS, including strategic and operational, legal, financial and reputational risks may also be prepared.

6.4 Notification

In accordance with the Data Protection Commissioner's "Personal Data Security Code of Practice" , all incidents in which personal data has been put at risk must be reported to the Office of the Data Protection Commissioner within 2 working days of SHS becoming aware of the incident.

All contact with the Data Protection Commissioner should be made through the Data Protection Officer.

6.5 Evaluation and Response

In the aftermath of a personal data security breach, a review of the incident may take place to ensure that the steps taken during the incident were appropriate and effective, and to identify any areas that may be improved in future, such as updating policies and procedures or addressing systematic issues if they arise.

7.0 ROLES & RESPONSIBILITIES:

7.1 Users

Each user of SHS's ICT resources is responsible for:-

7.1.1 Complying with the terms of this policy and all other relevant SHS polciies, procedures, regulations and applicable legislation.

7.1.2 Respecting and protecting the privacy and confidentiality of the information they process at all times.

7.1.3 Complying with instructions issued by the Data Protection Officer on behalf of SHS.

7.1.4 Reporting all misuse and breaches of this policy to their Senior Manager.

7.2 Senior Managers

In addition to each user's responsibilites, Senior Managers are directly responsible for:-

7.2.1 The implementation of this policy and all other relevant SHS policies within the business areas for which they are responsible.

7.2.2 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.

7.2.3 Consulting with the Data Protection Officer in relation to the appropriate procedures to follow when a breach of this policy has occurred.

7.3 ICT System Administrators & Developers

Each SHS System Administrator & Developer is responsible for:-

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

7.4 Data Protection Officer

In addition to the above responsiblities the Data Protection Oficer

7.4.1 Investigation any personal data breaches that are submitted.

7.4.2 If necessary inform the Data Protection Commissioner office of any data breaches.

8.0 ENFORCEMENT

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

8.2 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.