Document Control

Policy Title	Password Standards Policy
Policy Number	100
Owner	*ICT Manager*
Contributors	*Assistant to ICT Manager*
Version	2.0
Date of Production	24 Jul 2017
Review date	24 Jul 2019
Post holder responsible for review	*Senior Development Manager*
Primary Circulation List	E-Learning
Web address	http://elearning.sunbeam.ie/
Restrictions	None

Version Control

Version Number	Owner	Description	Circulation
2.0	Information & Communication Technology Manager	Review, Change and Update of Policy	E-Learning

1.0 POLICY:

Passwords are one of the primary mechanisms that protect critical SHS information systems and other resources from unauthorised use. Constructing secure passwords and ensuring proper password management are essential. Poor password management and protection could allow unauthorised access to the SHS Information Communication Technology (ICT) resources, which in turn could lead to the inappropriate disclosure and use of confidential or sensitive SHS information. The purpose of this policy is to provide clear guidance and present best practice for the creation of strong passwords, the management and protection of those passwords, and the frequency of change.

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

See appendix A for a list of definitions used in this policy.

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 Information Communication Technology (ICT) resources which include equipment, systems, and applications including cloud based applications and mobile telecommunications systems.
- All system users including contractors, agency staff and authorised third party commercial service providers and uses of SHS Information Communication Technology (ICT) resources.
- All connections to locally or remotely accessed SHS networks domains, cloud based or otherwise.

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

3.1.4 Ensure they comply with the latest version of this policy and all other relevant SHS polcies.

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 and any other system administration password(s) are secure and kept confidential.

3.4 ICT Manager

In addtion to the above responsiblities the ICT Manager ensures that all system developers/administrators (including third party contractors) who are responsible for developing systems for SHS, must ensure that their systems contain the following security features:

3.4.1 They must support authentication of individual users and not just groups.

3.4.2 They must not store passwords in clear text or in any easily reversible form

3.4.3 They must provide for some sort of role management, such that one user cannot take control of the functions of another without having a knowledge of the other users passwords where possible. If a password has to be disclosed for support or technincal reasons this must be the last resort and the password must be change immedialty after the support session is complete.

4.0 GUIDELINES:

All passwords must meet the following requirement:

4.1 What requires a password

Where technically feasible all SHS ICT resources must be protected by the use of a strong password.

4.2 Password Length

All passwords must be a minimum of 8 characters in length, regardless of whether the system enforces this or not. If a system is not capable of supporting 8 characters, then the maximum number of characters allowed by that system must be used.

4.3 Password Complexity

4.3.1 Passwords should contain a combination of letters (both upper and lower case, numbers (0-9) and special character.
Example of special characters: ! @ # $ ^ & * ( ) _ - + = [{] } ; : | . / ?

4.3.2 Passwords must not be left blank.

4.4 Password or part of a password must not contain:

1. Any common keyboard sequences
   For example: qwerty

2. Any part of the users user-name or email.

3. Any personal information related to a user
   For example: Date of Birth, Address, School, SHS personal number, car registration number, phone number.

4. A sequence of consecutive numbers or letters
   For example: 12345678, abcdefgh, abcd1234

5. Passwords that follow a common sequence or pattern.
   For example: Summer2016, Winter2016, Spring2017 etc.

6. Word that include information about your family, pets likes and dislikes
   For example: Hobbies, pet names, children names, nick names, favourite football club etc.

7. The following sequence of letters - *passwrd, passwd, pwrd, paswd, passwd*.

8. Common acronyms
   For example: aka, 24/7, asap, fyi, sob, tlc etc.

9. Any slang words
   For example: Dubs, agro, bling, Sham, etc.

10. Any names of people, places, organisation or fictional characters
    (For example: Jane999, Liverpool, LFC1234, ManUtd2016, JamesBond007)

4.5 Password History

No password may be re-used by a user within a 12-month period.

4.6 Password frequency of change

All users are required to change all SHS password specific to their various SHS User Account(s) to all the system(s) they have access to at least every 90 days regardless of whether the system enforces this or not.

4.7 Password security

- Users must not use the same password for multiple system or purposes.
- Each user is responsible for all activities performed on any SHS ICT device, information system or application while logged in under their individual access account and password.
- With the exception of generic / group access accounts users must only use user access accounts and passwords which have been assigned to them.
- Users must ensure all passwords except those used for generic / group access accounts are kept confidential at all times and are not shared with others including their co-workers or third parties. The following exception applies:
  - ICT support services; for support purposes only and only if there is no other option to resolve the issue. If a user has disclosed their password to a member of the ICT support services they must change that password once the support work is completed immediately.
- Users must not write down their password(s) on or near their computer device. However, in exceptional circumstances where a password has to be written down, the password must be stored in a secure locked place, which is not easily accessible to others.
- Users must not send their passwords within email messages unless the email message is encrypted.
- Users must change their passwords at least every 90 days or when advice to do so by their manager or a member of the ICT department.
- Users who suspect their password is known by others must change their password immediately.
- Users must not misuse their own or another user's password(s) and knowingly elevate their information system access/permissions privileges above those that they have been authorised to use.
- User must ensure all default passwords which are supplied by a vendor or by ICT support services for new SHS devices, systems and logins are changed at installation time or when first used.

5.0 ENFORCEMENT

5.1 SHS reserves the right to take such action as it deems appropirate against users who are in breach of this 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.

5.4 Breach of this policy by an employee may lead to disciplinary action.

Appendix A

Cloud: is a friendly way of describing web-based computing services that are hosted outside of your organization. When you use cloud-based services, your IT infrastructure resides off your property (off-premises), and is maintained by a third party (hosted), instead of residing on a server at your home or business (on-premises) that you maintain.

Information: Any data in an electronic format that is capable of being processed or has already been processed

Information Communication Technology (ICT) resources: Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment including mobile or cloud systems, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the SHS

Password: A string of characters that a user must supply in order to gain access to an ICT resource.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

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

System Administrators: The individual(s) charged by the designated system owner with the day to day management of SHS information systems. Also includes the SHS personnel and third parties who have been authorised to create and manage user accounts and passwords on these applications and systems.

System Developer: Any SHS personnel or third party commercial service providers who are responsible for developing electronic information systems and application for the SHS or its customers.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the SHS to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, client care and management services etc.) to SHS.

Users: Any authorized individual who uses the SHS ICT resources.