Aberdare Community School
Ysgol Gymunedol Aberdâr

Password Management Policy

Date Adopted	27th September 2023
Signature of Headteacher	
Signature of Chair of Governors	
Date to be reviewed	September 2025

PASSWORD MANAGEMENT POLICY

Review

This policy has been approved by the Technical Management Team and any amendments to it require the team's approval.

- Last approval: N/A
- Last review: N/A
- Next review: TBA

Overview

Protecting the schools computers, systems and data from unauthorised users is of paramount importance and passwords play an important role in this process. All users that have access to the computer systems must adhere to the password policy defined below in order to protect the security of the network, protect data integrity and protect computer systems.

Purpose

The purpose of this policy is to mandate a standard for the creation of strong passwords, their protection and frequency of change.
All users are issued with a permanent logon user id and initial personal password. The combination of userid and password enables logon and sign on to the schools networked computer systems.

Scope

This policy applies to employees, students, members, contractors, third party suppliers or anyone with an account (or any form of access that requires a password) on a school computer device or system. This includes system support staff and the use of privileged administrative passwords.

Definition

A Strong Password policy will be applied to all computer systems Strong& Weak passwords.

A **strong password** is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

A **weak password** is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

Risk

Passwords are the first line of defence for our ICT systems and together with the user id help to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

This policy aims to mitigate the risks stated above by enforcing a strong password policy.

Non-compliance with this policy could have a significant effect on the efficient operation of the school and may result in financial loss and an inability to provide necessary services.

Applying the Policy

Password Requirements

- Everyone must use strong passwords with a minimum standard of:
- At least six characters.
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)
- Must not be the same or contain part of your username within the password.
- Must not contain the first, middle or last name of your full name

Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never let anyone else access your account.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Never use the 'remember password' function.
- Do not use the same password for systems inside and outside of work.

Default passwords must also be changed immediately.

If you become aware, or suspect, that your password has become known to someone else, you must change it immediately.