Staff Password Policy

Overview

Passwords are an important aspect of network and computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire computer network of the School. As such, all school authorized account holders (including staff, students, agencies, with access to the school systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. All passwords are to be treated as sensitive, confidential school information.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all authorised account holders who have been provided an account on any computer system that is in use in the school.

Definitions

Every user should be aware of how to select and use strong passwords. Users must not use weak passwords.

Strong passwords:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g.,0!@#$%^&*()_+|~=\[]:";)
- Are at least six alphanumeric characters long.
- Should not be words in slang, dialect, jargon, etc.
- Should not be based on personal information, names of family, etc.

Weak passwords:

- Contain less than six characters
- Are found in a dictionary (English or foreign)
- Are common usage words such as: Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.
- Word, keyboard, or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards or followed by a digit (e.g., secret1)

Responsibilities

- All user-level passwords (e.g., windows login) must be changed every 6 months or earlier if compromised
- All passwords must be a minimum of six characters in length, contain both letters and numbers, and at least one capital or special character.
- Example password: Purple7

Implementation

After the initial password change staff will be notified by the system to change passwords at logon on the day their password reaches 6 months. Staff will not be able to use their previous password as this will be remembered by the system.

Last Reviewed: May 2021

Next Reviewed: May 2022