CBS Secondary School, Dungarvan.

Network Security Policy

As stated in our mission statement, Dungarvan CBS Secondary School is concerned with the overall well-being of the student that cares for the spiritual, intellectual, social, physical and emotional well-being of each student.

Staff at Dungarvan CBS must access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are a key part of IT's strategy to make sure only authorized people can access those resources and data.

All staff who have access to any of those resources are responsible for choosing strong passwords and protecting their log-in information from unauthorized people.

The purpose of this policy is to make sure all Dungarvan CBS resources and data receive adequate password protection. The policy covers all staff who are responsible for one or more account or have access to any resource that requires a password.

Password Creation:

All passwords should be reasonably complex and difficult for unauthorized people to guess. Staff should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. These requirements will be enforced with software when possible.
In addition to meeting those requirements, staff should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are equally bad from a security perspective.

A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase "This may be one way to remember" can become "TmB0WTr!".

Staff must choose unique passwords for all of their company accounts, and may not use a password that they are already using for a personal account.

All passwords must be changed regularly, with the frequency varying based on the sensitivity of the account in question. This requirement will be enforced using software when possible.

For computers connected via Active Directory Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords. The same will be done with Google Apps for Education and VSware for critical accounts that have access to sensitive information and the implementation of Two-Step-Authentication with be enforced for those accounts.

If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately.

Default Passwords — such as those created for new staff when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

Protecting Passwords

Staff may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

Staff may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

Staff should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.

Staff must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.

Staff may not use password managers or other tools to help store and remember passwords without IT's permission.

Policy Review:

This policy will be reviewed as necessary and particularly to comply with any relevant legislative changes.

Proposed by: _____ Chairperson: _____

Seconded by: _____ Date: _____