Marian College
Myrtleford

Marian College Password Policy for Students

Purpose

The purpose of this password policy is to establish guidelines for creating and maintaining strong passwords to ensure the security and confidentiality of sensitive information held by Marian College. A strong password policy is essential to safeguarding the College's data, resources, and systems from unauthorized access, misuse, and potential cyber threats.

Password Creation:

- Students are required to use a passphrase for their network account. It must contain a minimum of three random words, each word separated by a space
- The passphrase must be at least 14 characters long
- A combination of uppercase letters, lowercase letters, numbers and special characters are recommended but not required when using a strong passphrase
- Your passphrase should be unique and not used for other accounts or services
- Avoid using easily guessable information such as birthdates, family names, or common dictionary words. It must not contain words such as marian, mcm, welcome or any part of your name

Password Protection:

- Students are responsible for keeping their passwords confidential and not sharing them with anyone, including other students and family members
- Do not write down passwords on paper or electronic devices that are not secure
- If a password is suspected to be compromised or accidentally disclosed, students should immediately change their password
- Passwords should not be stored in web browsers or saved in clear text on devices
- Enable multi-factor authentication (MFA) where possible to add an extra layer of security

Password Renewal:

- Frequent password changes are no longer recommended. It is better to ensure that you create strong, unique passwords and only change your password when there is a suspicion of compromise or evidence of a security breach. A password audit will be performed regularly to check for any breaches

- Passwords cannot be reused when updating your password

Account lockout and login attempts:

- After five consecutive failed login attempts, your account will be locked for a period of 15 minutes

- If students suspect any unauthorized access attempts, they should report it immediately to the IT department

Policy Review:

- This password policy will be reviewed regularly to ensure it remains effective and relevant to the evolving security landscape

Updated August 2023