Password and Authentication Policy

**Organisation:** Holmview Primary  
 **Version:** 1.0  
 **Effective:** n/a  
 **Owner:** ICT Coordinator (with Principal oversight)  
 **Review cycle:** Annual, and after any major change or incident

# Table of Contents

[Table of Contents 1](#_Toc1092971536)

[Purpose 2](#_Toc1805474794)

[Scope 3](#_Toc40059731)

[Definitions 3](#_Toc1112429904)

[Policy Statements 3](#_Toc15686247)

[Minimum standards by account type 3](#_Toc579521202)

[Creation and Change 5](#_Toc200220273)

[Quality 5](#_Toc1505853195)

[Storage and Sharing 5](#_Toc288781424)

[Lockouts and Repeated Incorrect Attempts 5](#_Toc2052354912)

[Recovery and Resetting 6](#_Toc248416024)

[Legal 6](#_Toc1472111420)

[Exemptions 6](#_Toc6235902)

[Roles and Responsibilities 6](#_Toc617547164)

[Enforcement 7](#_Toc1478746317)

[Review 7](#_Toc1145031231)

# Purpose

The purpose of this document and policy is to protect school property, students and data. This will be achieved through setting clear expectations for passwords, passphrases and also multifactor authentication.

# Scope

This policy applies to the following:

* All Staff (teachers, admin, contractors, volunteers and student leaders)
* All students
* All school owned servers and systems (on premise, cloud hosted and third-party portals)
* All account types (privileged admin, user, system and temporary)

# Definitions

* **Password/Passphrase:** A secret key known only to the intended user. A passphrase is a longer sequence of words that will be used by non-students. The two words may be used interchangeably.
* **MFA:** Multi Factor Authentication, such as a password and text message or authenticator app.
* **Privileged Account:** Any account with elevated privileges such as a domain administrator, server administrator, etc.
* **System/Service Account:** A non-human use account that is used by services, scripts and other integrations such as monitoring

# Policy Statements

## Minimum standards by account type

Staff (teaching/admin staff that is not privileged)

* Must use MFA for any school related accounts and access.
* Passphrase >14 characters.
* Must include a number.
* Must include a special character.
* Can not contain an old passphrase.
* Must change passphrase every 12 months.

Privileged Admin Staff

* Must use MFA for any school related accounts and access with either a hardware key or authentication application on a separate device.
* Dedicated accounts without access to email or wifi sign in.
* Passphrase >16 characters.
* Must include a special character.
* Can not contain an old passphrase.
* Must include a number
* Can log in only from valid workstations and devices.
* Must change passphrase every 12 months.

Students

* Year 3-6: password of minimum 8 characters.
* P-2: device based sign in or other credential managed by mdm
* No MFA required for students, any sensitive information should be sent to parents via parent portal.

Parents/Guardians

* Password with at least 10 characters, passphrases are encouraged.
* Recommend MFA.

Service/Server/Script/Automated accounts

* Preferred to use key based login.
* Keys to be stored in a secure key vault/password management system.
* In the event a password must be used it is to be the following.
  + >24 characters.
  + Completely randomly generated with.
    - Numbers
    - Special characters
    - Capital letters
    - Lowercase letters
  + Changed every 12 months.
  + Stored in a secure location.

## Creation and Change

* New user accounts to be given a temporary one-time password that must be changed at the first login.
* Passwords must be changed in the event that there is a suspected compromise, breach or the device is stolen.
* Default vendor passwords must be changed before a device is deployed.

## Quality

As mentioned partly in the above sections passwords must pass certain quality checks for them to be secure. This section will detail other ways passwords will be made secure, including a blocklist.

* Common password checks should be in place along with a blacklist for things such as suberb/city, school name, mascot, keyboard walks, consecutive numbers, the word “password”, etc.
* Copy and paste password managers should be used for privileged admin staff in order to maintain password integrity and minimize mistakes.
* Password hints and other security questions must be disabled as a reset mechanism due to them being easily guessed by someone who knows the password setter.

## Storage and Sharing

* Passwords are never stored in plaintext.
* Password storage systems must use modern encryption and hashing algorithms.
* Passwords and other credentials are never sent via email, text message or written in easily readable places such as on a whiteboard.
* Password managers must have audit logging in place.

## Lockouts and Repeated Incorrect Attempts

* After three consecutive failed attempts to login to an account with a password or passphrase, the account must be locked for 10 minutes.
* Progressively larger delays should be put in place after more failures after the initial lockout.
* In the event of lockouts notifications will be sent to the appropriate personnel.

## Recovery and Resetting

* Staff are to use self-service password reset with MFA or see ICT staff.
* Students are to request a reset via their teacher or ICT staff.
* Parents are to use a self-service reset with MFA where applicable.
* All resets and recoveries are to generate log entries.

## Legal

* Aligns with ISO/IEC 27001 controls (Access Control & Authentication), ASD Essential Eight and privacy obligations under the Privacy Act 1988 and the Information Privacy Act 2009.
* Non-compliance may result in disciplinary action as well as access suspension.

## Exemptions

Any exemption must be approved by the principal in writing, include a compensation for the exemption and also be time limited pending review.

# Roles and Responsibilities

* **Principal:** Approves policy and exemptions, ensures the enforcement of the policy and necessary resources.
* **ICT Director:** Implements any necessary technical aspects, monitors logs for compliance and reports any abnormalities.
* **Business Manager/HR:** Ensures necessary account or personnel changes are made and communicated in a timely manner.
* **Staff:** Maintain strong and secure passphrases, report incidents and complete necessary training.
* **Students/Parents:** Keep passwords/credentials secure and private, and to notify the school in the event of a compromise.

# Enforcement

* Accounts and access may be suspended for breach of this policy.
* Serious breaches of this policy resulting in data breaches or similar will be escalated to the principal and where appropriate may also invoke external authorities as necessary.

# Review

This policy is to be reviewed annually and updated in order to match best practices. Furthermore, it may be reviewed in the event of any incidents or changes in technology or regulations.