Password Management Policy

© William College. All rights reserved

Document Version Control	
Document Title	Password Management Policy
Version	1
Reviewing Committee	Senior Leadership and Management Team
Approving Committee	Senior Leadership and Management Team
Policy Lead	IT Coordinator
Date of Last Review	May 2026
Date of Approval	May 2026
Date Effective from	June 2026
Date of Next Review	November 2027

© William College. All rights reserved

Table of Contents

1. Objective 3
2. Applicability 3
3. Policy Specification 3
3.1 General Password Standards 3
3.2 Institutional Password Standards 3
4. Mandatory Standards 4
4.1 Usernames 4
4.2 PINs 4
4.3 Password Complexity 4
5. Policy Review 4
6. Related Policies 4

© William College. All rights reserved

1. Objective

This document establishes the guidelines for creating secure passwords, safeguarding them, and ensuring they are updated regularly. Passwords, when paired with usernames, act as a fundamental layer of protection against unauthorised access to confidential systems, data, and facilities. They also play a key role in maintaining accountability through logging user activity for audit purposes.

2. Applicability

These standards apply to any user who accesses or manages accounts on any William College digital systems, services (such as email), secure environments, devices, or networks.

3. Policy Specification

3.1 General Password Standards

- Passwords must remain confidential and must not be shared with other users.
- Default credentials must be replaced immediately upon initial login. Users must set their own passwords when access is granted.
- Passwords must not be visible on screens, written down (e.g., sticky notes), or stored in easily accessible platforms (e.g., Slack, Outlook).
- All passwords must be stored in the system using encryption.
- Automatic login scripts containing passwords are not permitted.
- Passwords should not be saved in internet browsers.
- Employees must avoid using passwords from external platforms (e.g., Facebook) on internal systems.
- Passwords must be strong, incorporating uppercase and lowercase letters, numbers, and special characters. Longer passwords enhance security.
- Systems must retain password history to prevent reuse of the last 24 passwords.
- Passwords can be managed using an approved password manager.

3.2 Institutional Password Standards

- Identity verification is required before administrators reset passwords.
- Shared or group accounts are not allowed; any detected generic accounts must be disabled.
- Access for users who leave the organisation must be revoked immediately.
- Accounts that remain unused for three months must be disabled.
- Vendor accounts used for remote support must be activated only when needed and deactivated afterward.
- Vendor activity must be monitored during access periods.
- Multiple Factor Authentication (MFA) must be enabled wherever possible.
- System-level credentials (e.g., root, admin) must be updated at least every 90 days.
- If there is any suspicion of password or account compromise, the password must be changed without delay.

© William College. All rights reserved

4. Mandatory Standards

4.1 Usernames

Each member of staff must be assigned a unique username based on their first and last name.

- Username activity must be logged.
- Login screens must not display or allow selection of usernames.
- Usernames are considered internal data and must be protected accordingly.

4.2 PINs

PINs are numeric codes used for authentication.

- Easily guessed PINs such as “1234” or birth dates (e.g., 1102 for February 11) must be avoided.
- The use of words converted via mobile keypad mappings (e.g., “word” rendered as 9673) may be considered.
- PINs must remain confidential.
- Users are responsible for keeping their PINs secure and must change them immediately if compromised.

4.3 Password Complexity

Passwords must meet the following criteria:

- Minimum of eight (8) characters.
- Must include at least three of the following:
    - Uppercase letters (A–Z)
    - Lowercase letters (a–z)
    - Numbers (0–9)
    - Special characters (e.g., !, %, @)
- Must not be commonplace dictionary words (e.g. “password”, “football”, “open”).
- Must not be based on personal details (e.g., names of family, pets).
- Use of passphrases is highly encouraged. Example: “I love to play squash” becomes IL0ve2Play$qua£h.

5. Policy Review

This policy is reviewed every 18 months by the Senior Leadership and Management Team or sooner if required by regulatory changes or cybersecurity reviews.

6. Related Policies

- Acceptable Use of IT Services Policy
- Staff Bring Your Own Device (BYOD) Policy
- Starters and Leavers Checklist

© William College. All rights reserved