Planet Education Networks

Password Policy

Approval Control

Document Title:	Password Policy
Approving Body:	Senior Leadership Team (“SLT”)
Policy Lead:	Assistant IT Manager
Last Review:	September 2025
Effective From:	October 2025
Next Review:	September 2026

Planet Education Networks

Contents

1. Introduction and Purpose

Strong authentication is a critical defence against unauthorised access to Planet Education Networks' ("PEN") information assets. The purpose of this policy is to establish requirements for creating, managing, and protecting strong passwords and implementing robust authentication mechanisms across all organisational systems. This policy aims to protect the confidentiality, integrity, and availability of data by ensuring that only authorised individuals can access them.

2. Scope

This policy applies to all full-time and part-time employees, contractors, consultants, temporary staff, vendors, and any other individuals ("Users") who have been granted access to any Organisation-owned or managed information system, application, network device, or service. This includes, but is not limited to, email, learning platforms, administrative systems, and cloud services.

3. Password Requirements and Complexity

3.1. General User Passwords

- **Length:** Must be a minimum of 12 characters.
- **Complexity:** Must use a combination of at least three of the following four character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols.
- **Avoidance:** Must not be based on easily discoverable information such as usernames, family names, pets, or common dictionary words.
- **Passphrases:** The use of strong, memorable passphrases is strongly encouraged (e.g., BlueSky$Flying-High2024!).

3.2. Privileged/Administrative Accounts

- **Length:** Must be a minimum of 16 characters and adhere to the complexity rules above.
- **Usage:** Must only be used for administrative tasks and not for daily-use activities like email or web browsing.

3.3. Password Screening

- All new or changed passwords will be screened against a list of known compromised passwords from previous data breaches and must not be a match.

4. Password Management and Protection

4.1. Confidentiality

- Passwords must never be shared with anyone, including colleagues, assistants, or family members. The only exception is for provision to a designated, secure enterprise password manager.

4.2. Storage

- Passwords must never be stored in clear text. This includes on paper, in unencrypted files (e.g., Word documents, Excel spreadsheets), emails, instant messaging platforms (e.g., Slack, Teams), or notes on mobile devices.
- The use of an approved enterprise password manager is mandatory for storing and managing work-related credentials.

4.3. Re-Use and History

- Passwords used for Organisation systems must not be used for personal accounts (e.g., social media, personal banking).
- A password history of at least the last 10 passwords shall be maintained to prevent immediate re-use.

4.4. Change Frequency

- User passwords will not be forced to expire arbitrarily. Passwords must be changed immediately if there is any suspicion of compromise.
- Passwords for privileged/administrative accounts must be changed at least every 90 days or following any personnel change in the team with access.

5. Account Security Controls

5.1. Multi-Factor Authentication ("MFA")

- MFA is mandatory for all remote network access (VPN), cloud administrative consoles, and all privileged user accounts.
- MFA is strongly recommended and should be enabled on all systems where it is available, especially for email and other core business applications.
- Where supported, phishing-resistant MFA (e.g., FIDO2 security keys) is the preferred standard for high-risk accounts.

5.2. Account Lockout and Session Management

- User accounts will be automatically locked after 10 failed login attempts within a 30-minute period. Accounts will remain locked for 30 minutes or until unlocked by the IT Helpdesk.
- System and application sessions must lock after 15 minutes of inactivity. Sessions for administrative systems must lock after 5 minutes of inactivity, requiring re-authentication.

5.3. Unique Identifiers

- Each user must be assigned a unique username (user ID) for accountability. Usernames must not be displayed on login screens to unauthorised persons.

6. Administrative Responsibilities

6.1. Account Lifecycle Management

- User accounts must be created following a formal, authorised request.
- Access for terminated users must be revoked immediately upon notification from HR.
- Inactive user accounts (e.g., no login for 90 days) must be disabled and, after a further review period, deleted.

6.2. Password Resets

- The IT Helpdesk must verify the identity of a user through a defined and secure process before performing any password reset. Resets must never be performed based on an email request alone without secondary verification.

6.3. Default and Generic Passwords

- All default passwords on systems, applications, and network equipment must be changed before being placed into production.

- The use of shared or generic accounts (e.g., "admin", "guest") is prohibited. Where a technical exception is unavoidable, the account must be highly restricted, closely monitored, and its password changed frequently.

7. Special Cases

7.1. Vendor and Remote Support Accounts

- Any temporary accounts created for vendors or remote support must be enabled only for the specific period required and disabled immediately upon completion of the work. Their use must be monitored and logged.

7.2. **Personal Identification Numbers** (“PINs”)

- PINs used for authentication (e.g., for mobile devices, encryption) must be a minimum of 6 digits and must not be sequential (e.g., 123456) or repetitive (e.g., 111111).
- PINs must be treated as confidential information and must not be shared.

8. Compliance and Enforcement

Compliance with this policy is mandatory. Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and may face legal action in the case of gross negligence or malicious intent. The IT Department will utilise technical measures to enforce these requirements where possible and will conduct periodic audits to ensure compliance.

9. Related Documents

- Acceptable Use Policy
- Access Control Policy
- Bring Your Own Device (BYOD) Policy
- Endpoint Detection and Response (EDR) Policy
- Information Security Awareness Policy
- Starters and Leavers Checklist