Planet Education Networks

Access Control Policy

Approval Control

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

Planet Education Networks

Contents

1. Purpose

This policy establishes the framework for access control at Planet Education Networks ("PEN") to ensure that information assets are protected from unauthorised access while enabling authorised users to perform their legitimate functions. The policy implements the principles of least privilege and need-to-know across all systems and data.

2. Scope

This policy applies to all PEN employees, contractors, vendors, and any other individuals who require access to the PEN's information systems, networks, data, or physical premises.

3. Principles of Access Control

3.1. **Least Privilege:** Users shall be granted only the minimum access rights necessary to perform their authorised tasks.

3.2. **Need-to-Know:** Access to information is restricted to individuals who require it for legitimate business purposes.

3.3. **Segregation of Duties:** Critical functions shall be divided among multiple individuals to prevent conflict of interest and reduce fraud risk.

3.4. **Defence in Depth:** Security shall be implemented through multiple complementary controls.

3.5. **Accountability:** All access must be attributable to a unique individual.

4. Roles and Responsibilities

4.1. IT Department

- Implement and maintain technical access control systems
- Process authorised access requests and modifications
- Manage user authentication systems
- Conduct regular access reviews and audits
- Maintain access control logs

4.2. Asset Owners

- Classify information assets according to sensitivity
- Authorise access requests based on business need
- Review and validate existing access rights quarterly

4.3. Line Managers

- Initiate access requests for team members
- Ensure timely removal of access for leavers
- Justify privileged access requirements

4.4. All Users

- Protect authentication credentials
- Use access only for authorised purposes

- Report suspicious activity or access violations
- Complete mandatory security awareness training

5. User Access Management

5.1. User Registration

- All users must be assigned unique identifiers
- Generic accounts are prohibited unless specifically justified and approved
- Access rights must be based on role requirements
- The principle of segregation of duties must be enforced during account creation

5.2. Access Review

- User access rights must be reviewed by asset owners quarterly
- Privileged accounts must be reviewed by IT monthly
- Inactive accounts must be disabled after 30 days

5.3. Access Removal

- Access rights must be removed upon termination of employment
- Line managers must notify IT of leavers on their last working day
- Accounts must be disabled immediately, with deletion after 90 days
- For high-risk terminations, access must be revoked before notice is given

6. Privileged Access Management

- Privileged accounts must be separate from standard user accounts
- Privileged access requires written approval from department head and IT Manager
- All privileged access must be logged and monitored
- Privileged account usage must be limited to specific administrative tasks
- Session recording must be enabled for critical system access

7. Network and Remote Access

7.1. Network Access

- Non-PEN devices require specific approval before network connection
- All network access must be authenticated
- Third-party access must be reviewed quarterly

7.2. Remote Access

- Multi-factor authentication (MFA) is mandatory for all remote access
- VPN connections must use approved encryption standards
- Remote access software must be disabled when not required
- All remote access must be logged and monitored

8. Authentication Requirements

8.1. Password Standards

- All passwords must comply with the Password Policy
- Initial passwords must be changed on first use
- Password characters must be hidden during entry

8.2. Multi-Factor Authentication

MFA is mandatory for:

- All remote network access (VPN)
- All administrative accounts
- Access to sensitive data repositories
- Cloud-based management consoles

8.3. System Access Controls

- Account lockout after 5 failed login attempts
- Session timeout after 15 minutes of inactivity
- No system identifiers displayed before successful authentication
- Logon time limited to 15 minutes maximum

9. Physical Access Controls

- Access to offices controlled by swipe card system
- All visitors must be signed in and escorted
- Data centre access restricted to authorised personnel only
- Physical documentation secured in locked cabinets
- CCTV monitoring in operation as per CCTV Policy
- Staff must display identification at all times

10. Compliance and Enforcement

- Compliance with this policy is mandatory for all users
- Access control violations may result in disciplinary action
- Regular audits will verify compliance with this policy
- Systems not compliant may be disconnected from the network

11. Related Policies

- Acceptable Use Policy
- Password Policy
- Data Protection and Confidentiality Policy
- Bring Your Own Device (BYOD) Policy
- Information Security Awareness Policy