PEN
Planet Education Networks

Bring Your Own Device (BYOD) Policy

Approval Control

Document Title:	Bring Your Own Device (BYOD) Policy
Approving Body:	Senior Leadership Team (“SLT”)
Policy Lead:	Assistant IT Manager
Last Review:	March 2025
Effective From:	April 2025
Next Review:	March 2026

Contents

1. Purpose

The purpose of this policy is to define the conditions for the Bring Your Own Device (BYOD) program at Planet Education Networks ("PEN"). This program allows eligible staff to use personally owned devices to access the PEN's IT resources and data in a secure manner that protects both institutional data and individual privacy, in compliance with the UK GDPR and Data Protection Act 2018.

2. Scope

This policy applies to all PEN staff members who choose to participate in the BYOD program. It covers any personally owned smartphone, tablet, or laptop used to access, process, or store PEN data, including but not limited to email, calendar, documents, and network resources.

3. BYOD Program Principles

- The BYOD program operates on a principle of shared responsibility: PEN provides secure access to resources while participants maintain their devices in compliance with PEN security requirements.
- Participation in the BYOD program is voluntary and requires formal approval.
- All use of personal devices for PEN purposes must comply with PEN's Acceptable Use Policy.

4. Security Requirements

4.1. Access Controls

- Devices must be protected with a secure screen lock (PIN, password, or biometric) with a maximum 5-minute inactivity timeout
- The same device must not be used by other household members to access PEN resources
- Rooted (Android) or jailbroken (iOS) devices are strictly prohibited
- The device must be enrolled into the company Mobile Device Management solution

4.2. Software Maintenance

- Operating systems and applications must be kept current with the latest security updates
- PEN-approved antivirus software must be installed and kept updated (provided by the PEN)
- Device firewalls must be enabled where available

5. Data Protection and Privacy

5.1. Data Segregation

PEN data (including personal data and confidential information) should not be stored in personal device areas.

5.2. Privacy Protection

PEN will not:

- Monitor personal use, location, or web browsing history
- Access personal data such as photos, messages, or personal email addresses
- Inspect personal content during device offboarding

5.3. Incident Reporting

Any loss, theft, or suspected security compromise of a BYOD device must be reported to the IT Department immediately.

6. Remote Management and Data Wipe

6.1. Selective Wipe

PEN reserves the right to remove access to PEN data in the event of:

- Termination of employment
- Device loss or theft
- Security policy violations
- Device non-compliance with security requirements

6.2. Full Device Wipe

A complete device wipe (including personal data) will only be considered as a last resort in cases of severe, immediate security threats that cannot be contained. Every reasonable effort will be made to alert the employee before performing a full wipe.

7. Financial Responsibilities

7.1. The employee is responsible for all costs associated with their personal device, including:

- Purchase, maintenance, and repair costs
- Mobile data plans and call charges
- Roaming charges and excess usage fees

7.2. PEN will provide and cover costs for:

- Mandatory security software required by the BYOD program
- Support for PEN application configuration

8. Termination of Participation

Upon termination of employment or withdrawal from the BYOD program, the employee must present the device to IT for secure removal of PEN data. This process is automated and only removes PEN applications and data.

9. Compliance and Enforcement

Failure to comply with this policy may result in suspension of BYOD privileges and/or disciplinary action in accordance with PEN procedures. Serious violations may lead to termination of employment and/or legal action.

10. Approval Process

Employees wishing to participate in the BYOD program must:

- Complete a BYOD request form with their line manager
- Read and acknowledge this policy and related security policies

11. Related Policies and Documents

- Acceptable Use Policy
- Data Protection and Confidentiality Policy

- Password Policy
- Endpoint Detection and Response (“EDR”) Policy
- Information Security Awareness Policy
- Starters and Leavers Procedure