Planet Education Networks

Acceptable Use Policy

Approval Control

Document Title:	Acceptable Use Policy
Approving Body:	Senior Leadership Team ("SLT")
Policy Lead:	Assistant IT Manager
Last Review:	April 2025
Effective From:	May 2025
Next Review:	April 2026

Planet Education Networks

Contents

1. Introduction and Purpose

Planet Education Networks ("PEN") provides IT resources (including computers, networks, software, internet access, and email systems) to support its educational, research, and administrative missions. This policy outlines the standards for acceptable use of these resources.

The purpose of this policy is to:

- Ensure the integrity, security, and reliability of PEN's IT assets.
- Protect PEN and its users from legal and reputational harm.
- Promote a responsible and secure digital environment for all members of our community.

This policy applies to all users of PEN's IT systems, including staff, faculty, contractors, and authorised visitors.

2. General Principles

PEN's resources are provided for purposes directly related to its academic and operational activities. Use of these resources is a privilege, not a right, and is subject to this policy. All users are expected to:

- Act responsibly and ethically.
- Respect the rights and privacy of others.
- Comply with all applicable laws and PEN policies, including the Data Protection and Confidentiality Policy.
- Understand that they may be held accountable for their conduct.

3. Acceptable Use

Use of IT systems is considered acceptable when it is for purposes related to the user's role at PEN, such as:

- Administrative and business operations.
- Official communication between staff and the PEN.
- Reasonable personal use that is lawful, minimal, does not interfere with the user's duties or others, and does not incur significant additional cost to PEN.

4. Unacceptable Use

The following activities are strictly prohibited. This list is not exhaustive but provides examples of unacceptable behaviour.

4.1. Illegal or Malicious Activity

- Accessing, creating, storing, or transmitting illegal material (e.g., copyrighted software/media without a licence, obscene material, defamatory content).
- Engaging in hacking, cracking, or any attempt to compromise system security.
- Introducing malware (viruses, ransomware, spyware) into PEN's network.
- Conducting fraudulent or malicious activities.

4.2. Security Violations

- Sharing your login credentials (username/password) with anyone else.

- Attempting to access another user's accounts, files, or data without explicit authorisation.
- Using PEN's systems to gain unauthorised access to any other system or network.
- Disabling or bypassing any security or monitoring controls installed by the IT department.

4.3. Harassment and Misuse of Communication Systems

- Using email, messaging systems, or social media to harass, bully, threaten, or discriminate against others.
- Sending unsolicited mass emails (spam) or chain letters.
- Impersonating another individual or PEN itself in electronic communications.
- Forging email headers or otherwise attempting to hide the origin of a message.

4.4. System Integrity and Performance

- Installing unauthorised software or hardware on PEN-owned devices or networks.
- Engaging in activities that place an excessive load on network resources (e.g., high-volume data mining, running servers for non-academic purposes without authorisation) that hinders system performance for others.
- Deliberately degrading or disrupting the performance of IT systems.

4.5. Data Protection and Confidentiality

- Processing, storing, or transmitting personal data in violation of PEN's Data Protection and Confidentiality Policy.
- Sending sensitive or confidential data (e.g., student records, staff information) via unencrypted email without a lawful basis and appropriate safeguards.
- Storing PEN-confidential data on personal devices or unauthorised cloud services (e.g., personal Google Drive, Dropbox) without explicit permission and appropriate security measures.

5. Privacy and Monitoring

While PEN respects user privacy, users should have no expectation of privacy in their use of PEN's IT resources. PEN reserves the right to:

- Monitor, log, and audit all activity on its IT systems and networks to ensure policy compliance, maintain system integrity, and investigate security incidents.
- Access, review, and disclose the contents of user accounts, files, and communications where there is a legitimate business need, a suspected policy violation, or a legal requirement (e.g., a Subject Access Request, court order).

Such activities will be conducted in accordance with the Data Protection Act 2018 and the UK GDPR.

6. Use of Personal Devices (BYOD)

Staff using personal devices (laptops, tablets, phones) to access PEN systems or data (e.g., email, network drives) must ensure those devices are:

- Protected with up-to-date anti-virus software and security patches.
- Secured with a password or PIN.

- Used in compliance with all aspects of this policy, the Data Protection and Confidentiality Policy and the Bring Your Own Device Policy.

PEN is not liable for loss or damage to personal devices.

7. Intellectual Property

Users must respect copyright and intellectual property laws. Unauthorised copying, sharing, or distribution of copyrighted software, music, videos, or texts using PEN resources is prohibited.

8. Consequences of Violation

Violations of this policy may result in disciplinary action, which can include but is not limited to:

- Temporary or permanent revocation of IT access privileges.
- Academic penalties (for students).
- Disciplinary action under the staff grievance and disciplinary procedure, up to and including dismissal.
- Legal action or reporting to relevant law enforcement agencies.

9. Policy Agreement

By using PEN's IT resources, all users acknowledge that they have read, understood, and agree to comply with this policy.

For Questions or to Report a Security Incident:

Please contact the IT Help Desk at it_infrastructure@pengroup.com or your line manager. Suspected policy violations can be reported anonymously through PEN's confidential reporting procedure.