Planet Education Networks

Information Security Awareness Policy

Approval Control

Document Title:	Information Security Awareness Policy
Approving Body:	Senior Leadership Team ("SLT")
Policy Lead:	Assistant IT Manager
Last Review:	January 2025
Effective From:	February 2025
Next Review:	January 2026

Planet Education Networks

Contents

1. Purpose

The purpose of this policy is to establish a formal and ongoing Security Awareness Programme Planet Education Networks ("PEN"). This programme is designed to equip all staff and relevant third parties with the knowledge to recognise, avoid, and report security threats, ensuring they understand their responsibilities in safeguarding the confidentiality, integrity, and availability of PEN's information assets. The ultimate goal is to foster a robust security-conscious culture across the organisation.

2. Scope

This policy applies to all individuals who access, use, or manage PEN's information assets, including but not limited to: all full-time and part-time employees, contractors, temporary staff, and third-party vendors.

3. Responsibilities

3.1. **SLT** is responsible for:

- Championing the importance of the Security Awareness Programme.
- Providing adequate resources for its development and delivery.
- Holding department heads accountable for their teams' participation and compliance.

3.2. **IT Department** is responsible for:

- Developing, implementing, and maintaining the Security Awareness Programme.
- Selecting or developing training content that is relevant, engaging, and up-to-date with the current threat landscape.
- Tracking completion rates and reporting on the programme's effectiveness to the SLT.
- Disseminating security bulletins and alerts regarding emerging threats.

3.3. **HR and Department Heads** are responsible for:

- Ensuring new starters are enrolled in security awareness training as part of the onboarding process.
- Facilitating the participation of their team members in mandatory training.
- Supporting enforcement by managing any disciplinary procedures arising from policy violations.

3.4. **All Users** are responsible for:

- Completing all mandatory security training within the stipulated timeframes.
- Adhering to all PEN information security policies and procedures in their daily work.
- Remaining vigilant and reporting any suspected security incidents or weaknesses promptly via the correct channel.

4. The Security Awareness Programme

The policy shall be supported by a living Security Awareness Programme that includes, but is not limited to, the following components:

4.1. Onboarding Training:

All new joiners must complete a mandatory security awareness training module prior to being granted access to any PEN information systems or data.

4.2. Ongoing and Annual Training:

- All users must complete annual refresher security awareness training.
- Additional, targeted training may be required for roles with specific risk profiles (e.g., Finance staff, HR, IT Administrators).

4.3. Phishing Awareness:

- The programme will include simulated phishing campaigns to provide practical, experiential learning and to measure the organisation's resilience to email-based attacks.
- The results will be used for positive reinforcement and further targeted education, not punitive measures for failure.

4.4. Content and Communication:

- Training content must be kept current and address relevant threats, including phishing, social engineering, malware, data protection (UK GDPR), secure remote working, and physical security.
- The IT Security Team will regularly communicate security tips, bulletins, and updates on new threats to all staff.

4.5. Records and Evidence:

- Completion of all mandatory training must be recorded and tracked. These records shall be maintained for audit and compliance purposes for a minimum of three years.

5. Policy Acknowledgement and Compliance

All users are required to formally acknowledge that they have read, understood, and will comply with all PEN information security policies, including this one, as a condition of their access to PEN's information resources.

6. Enforcement

Any user found to have violated this policy may be subject to disciplinary action, in accordance with PEN's disciplinary procedures, up to and including termination of employment or contract. Repeated failure to complete mandatory training will be considered a violation of this policy.

7. Related Policies and Legislation

- Acceptable Use Policy
- Data Protection and Confidentiality Policy
- Access Control Policy
- Password Policy
- Endpoint Detection and Response (EDR) Policy
- Bring Your Own Device (BYOD) Policy
- Starters and Leavers Checklist
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018