Planet Education Networks

Web Filtering and Monitoring Policy

Planet Education Networks

Approval Control

Document Title:	Web Filtering and Monitoring Policy
Approving Body:	Senior Leadership Team ("SLT")
Policy Lead:	Assistant IT Manager
Last Review:	August 2025
Effective From:	September 2025
Next Review:	August 2026

Planet Education Networks

Contents

1. Introduction

Web filtering is a crucial security measure at Planet Education Networks Ltd ("PEN") to ensure a safe and productive environment for staff and visitors. It is designed to protect users from accessing harmful, malicious or inappropriate content, whilst upholding academic freedom and maintaining the integrity of PEN's IT systems.

The policy outlines clear guidelines and procedures for implementing and managing web filtering and monitoring measures at PEN. It's objectives are to:

- Protect users from exposure to harmful or inappropriate content.
- Safeguard the integrity and security of PEN's IT infrastructure.
- Ensure compliance with legal and regulatory requirements, including the prevent duty.
- Promote responsible and ethical internet use within the PEN community.

2. Purpose

This policy establishes a framework to effectively manage web filtering and monitoring at PEN in accordance with its statutory obligations.

By enforcing these measures, PEN aims to protect its users from accessing malicious content whilst balancing academic freedom and operational integrity.

3. Scope

This Policy applies to all users of PEN's systems and infrastructure, including its employees, contractors, and authorised users within client institutions who access services under PEN's management.

PEN provides web filtering and monitoring services to its client institutions. Students and staff of those institutions are covered by their respective institution's policies, which incorporates the technical controls implemented by PEN.

PEN retains user activity log information for purposes, including but not limited to, network monitoring, cybersecurity, operational management and safeguarding.

The logged information includes firewall traffic and website access logs, details of the user identity (where available), source and destination IP addresses, the type of traffic, intrusion prevention information and website classification.

4. Storage, Retention and Use of Logged Information

All website activity logs are securely stores on PEN's encrypted internal services, accessible only to authorised IT personnel. Retention periods align with GDPR guidelines, to ensure data is only kept for as long as necessary for safeguarding, security and operational purposes.

Web activity logs are retained for a period of 30 days, after which they are securely deleted, unless retention is requirement for ongoing investigations or compliance purposes. Logs are reviewed periodically for security, auditing, network optimisation and compliance checks.

Access to this data is strictly limited to involving security incidents, policy violations or formal requests from compliance or safeguarding teams.

In line with PEN's Data Retention Policy, secure data disposal procedures ensure that all logs and other stored data are irreversibly deleted after the retention period.

5. Implementation of Web Filtering and Monitoring

PEN uses standalone devices to manage web filtering and monitoring.

The system filters online content using predefined and regularly reviewed categories, blocks access to malicious or inappropriate material, monitors and logs web activity to support safeguarding and security compliance, identifies attempts to access restricted websites, and helps protect staff and students in line with online safety and Prevent Duty requirements.

6. Determination and Review of Malicious Content

The IT Department maintains a categorised list of restricted content, which is reviewed quarterly.

Requests for access to restricted content for legitimate academic purposes will be evaluated by the IT department in collaboration with relevant client departments.

7. Special Considerations for Academic Research

Academic staff requiring access to sensitive content for legitimate purposes must submit a request to the IT Department. All requests will be logged, and access granted (after evaluation) under controlled conditions.

8. Exceptions Request

Users who believe that access to a specific website has been unjustly restricted may submit an appeal to the IT Department. The appeal should include justification for access and any supporting documentation, such as academic research requirements. Appeals are reviewed within 5 working days by the IT department in consultation with the relevant client departments and senior management (if required).

If the appeal is upheld, access will be granted under controlled conditions, and the decision will be logged for future reference.

If denied, users will be provided with a formal explanation by email and an escalation process to senior management for final review will be available if necessary.

9. Acceptable Use and Compliance

All users must comply with PEN's IT Acceptable Use Policy, under which the following actions are prohibited:

Content	Explanatory Note
Malware/Hacking	Promotes the compromising of systems, including anonymous browsing, filter by pass tools and sites hosting malicious content.
Extremism	Encourages or glorifies terrorism, radicalisation or hate-driven ideologies.
Self-Harm	Promotes self-harm, suicide or dangerous challenges that could lead to injury.
Piracy and Copyright Infringement	Facilitates illegal downloading, streaming or distribution of copyrighted material.
Violence and Gore	Displays excessive violence, graphic imagery or content that could be disturbing.
Drugs and Substance Abuse	Promotes the use, sale or manufacturing of illegal drugs and substances.
Gambling	Encourages online betting, casinos and other gambling-related activities.

Pornography and Adult Content	Contains explicit sexual content or promotes adult services.
Hate Speech	Spreads discrimination, bigotry or incites violence against individuals or groups.
Weapons and Firearms	Promotes the use, sale or manufacturing of illegal firearms or weapons.
Phishing and Fraud	Engages in deceptive practices to steal personal information or financial credentials.
Illegal activities	Encourages or facilitates illegal activities including fraud, theft and exploitation.
Proxy and VPN Services	Attempts to bypass network security using VPNs, proxies or other anonymising tools.
Online Harassment and Cyberbullying	Facilitates cyberbullying, threats, doxxing or other forms of online harassments.
Misinformation	Disseminates false information or misleading content that can cause harm or deception.
Social Networks	Restricts access to social media platforms that can be distracting and may pose security or privacy risks.
Google Ads and Targeted Advertising	Blocks intrusive online advertising, including personalised tracking ads to prevent data collection and privacy invasion.

10. Accountability and Risk Management

Roles and Responsibilities

The IT Department is responsible for implementing and managing web filtering technology, reviewing logs and ensuring compliance with this policy.

PEN senior management is responsible for overseeing compliance with this policy, reviewing risk assessments and ensuring that appropriate actions are taken to mitigate risks.

Risk Assessment and Reporting

Risks associated with web filtering and monitoring are assessed annually. Any risks identified are documented and reported to PEN Senior Management for review and potential mitigation strategies.

11. Incident Reporting Procedures

Any suspected breach or unauthorised attempt to access restricted content must immediately be reported to the IT Department with no further action required from the user.

The IT Department will conduct an initial investigation and, if necessary, escalate significant incidents to Senior Management. If a critical security or safeguarding issues is identified, immediate action will be taken, and the appropriate escalation procedure will be followed.

For serious incidents requiring external intervention (such as law enforcement), reports will be made in accordance with PEN's Data Protection Policy.

12. Data Protection and Privacy

Web activity logs will be stored securely and accessed only by authorised personnel. PEN will comply with the Data Protection Act 2018 and UK GDPR to ensure responsible handling of user data. Secure data

disposal procedures will be implemented to ensure that logs and other stored data are irreversibly deleted in accordance with PEN's Data Protection and Confidentiality Policy.

13. Review and Compliance

This policy will be reviewed annually to align with evolving cybersecurity threats and legal standards. PEN staff receive training on the importance of web filtering and monitoring as a part of their induction.

In the case of any changes to the regulatory framework, PEN reserves the right to amend this policy at any time.

For further details, please contact the IT Department.

14. Related Policies and Legislation

- Data Protection and Confidentiality Policy
- Access Control Policy
- Endpoint Detection and Response (EDR) Policy
- Bring Your Own Device (BYOD) Policy
- Data Protection Act 2018 and UK GDPR
- Counter Terrorism and Security Act 2015
- Higher Education and Research Act 2017