Planet Education Networks

CCTV Policy

Approval Control

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

Planet Education Networks

Contents

1. Introduction and Purpose

Planet Education Networks ("PEN") uses Closed-Circuit Television ("CCTV") and other image capture systems to monitor its premises. The primary purposes of this surveillance are:

- To ensure the health, safety, and security of our staff, students, and visitors.
- To protect PEN's property, assets, and facilities from damage, theft, and vandalism.
- To prevent, deter, and detect crime and support the investigation of incidents.
- To assist law enforcement agencies in the apprehension and prosecution of offenders.

This policy governs the management, operation, and use of the CCTV system to ensure it is used responsibly, effectively, and in full compliance with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

2. Scope

This policy applies to all CCTV systems operated by PEN on its premises, including cameras, recording equipment, and stored footage. It applies to all staff, students, contractors, and visitors to PEN sites.

CCTV cameras are strategically installed in and around PEN's premises. Monitored areas typically include:

- Main entrances and exits.
- Reception areas, lobbies, and hallways.
- Other designated locations identified as requiring monitoring for safety and security purposes.

The areas covered by CCTV are clearly indicated with visible signage. Monitoring will not be conducted in areas where individuals have a reasonable expectation of privacy, such as restrooms, changing rooms, or private offices.

3. Principles of Lawful Use

PEN justifies its use of CCTV under the 'legitimate interests' legal basis as defined by the UK GDPR. We are committed to ensuring that our use of surveillance is:

- **Necessary:** Used only for the specific purposes outlined in this policy.
- **Proportionate:** The intrusion on privacy is balanced by the security benefits.
- **Transparent:** Clear signage and this policy inform individuals of the surveillance.

CCTV will not be used for continuous monitoring of employee performance, nor for any other purpose unrelated to the stated security and safety objectives.

4. Recording, Storage and Retention

- **Recording:** Designated CCTV cameras will record footage continuously.
- **Retention:** Recorded footage will be stored for a maximum period of 30 days**,** after which it is automatically overwritten, unless it has been specifically retained for an ongoing investigation or legal proceedings.
- **Storage and Security:** All footage is stored digitally on encrypted hard drives located within a secure, access-controlled server room. Physical access to the recording equipment is restricted to authorised IT personnel.

5. Access Control and Disclosure

5.1. Authorised Access

- Live viewing and access to recorded footage is strictly limited to: Authorised IT Personnel for system maintenance and troubleshooting.
- Designated Security Personnel for the investigation of security incidents.
- Senior Management on a strict need-to-know basis for specific, legitimate incidents.

5.2. Disclosure to Third Parties

CCTV footage will only be disclosed to third parties under the following conditions:

- In response to a valid, written request from a law enforcement agency.
- Where required by law, such as pursuant to a court order.
- Where necessary for the establishment, exercise, or defence of legal claims.
- With the explicit consent of any identifiable individual(s) in the footage.

5.3. Audit Trail

All instances of access to, or disclosure of, CCTV footage must be recorded in a dedicated Access Log managed by the IT Department. The log must include the date, time, name of the person accessing, reason for access, and details of any footage copied or disclosed.

6. Individual Rights (Subject Access Requests)

Individuals have the right to request access to CCTV footage of themselves (a Subject Access Request). All such requests must be submitted in writing to the contact details provided in the signage and this policy. PEN will process requests in accordance with its Data Protection Policy and may need to obscure images of other individuals to protect their privacy rights.

7. Signage

Clear and visible signs will be displayed at all entrances to the premises and in key locations within monitored areas. The signage will state that CCTV is in operation and provide contact details (it_infrastructure@pengroup.com) for enquiries related to data protection.

8. System Management and Security

- The CCTV system will be regularly maintained and checked to ensure its operational effectiveness and image quality.
- All exported footage (e.g., for law enforcement) must be transferred using encrypted, password-protected devices and securely deleted once its specific purpose is fulfilled.

9. Staff Training

PEN will ensure that all staff responsible for operating the CCTV system, handling footage, or responding to access requests receive comprehensive training on this policy, data protection law, and the ethical use of surveillance systems. Regular refresher training will be provided.

10. Policy Violations and Complaints

Any breach of this policy, including unauthorised access, copying, or misuse of CCTV footage, will be treated as a serious matter and may result in disciplinary action, up to and including dismissal, and/or legal proceedings.

Complaints or enquiries regarding the operation of PEN's CCTV system should be directed to: it_ifrastructure@pengroup.com.

11. Related Documents

- Data Protection and Confidentiality Policy
- Information Security Awareness Policy