

Brunel University London CCTV Policy July 2026 V3

CHANGE LOG

- 03/2024: V1 – New policy – Terry Vass
- 09/2024: Approved at IAC – Terry Vass
- 04/2025: V2 – Updated to reflect Martyn’s Law compliance – Terry Vass
- 07/2026: Enhanced Security and Cyber Security controls – Terry Vass

1. Introduction

Brunel University London recognises the importance of maintaining a safe and secure environment for its students, staff, visitors, and property. Closed Circuit Television (CCTV) plays a vital role in enhancing security and safety across the campus. This policy outlines the principles, procedures, and responsibilities governing the use of CCTV systems within Brunel University London premises, satellite locations, and the use of Body Worn Video (BWV).

2. Purpose

The purpose of this policy is to:

- Ensure the effective and lawful use of CCTV systems to enhance security and safety.
- Protect the privacy and rights of individuals in accordance with relevant legislation.
- Define the roles and responsibilities concerning the operation, management, and monitoring of CCTV systems.
- Provide guidelines for the storage, access, and retention of CCTV footage.

2.1 Objectives

The primary objectives of our CCTV installations are:

- **Protection of Stakeholders and Assets:** Safeguarding the well-being of our staff, students, visitors, and University assets.
- **Crime Prevention and Detection:** Deterring criminal activity and supporting the investigation of disciplinary offences in accordance with University procedures.
- **Apprehension and Prosecution of Offenders:** Using CCTV images and data as evidence in criminal and civil proceedings.
- **Premises Security Monitoring:** Enabling timely responses to incidents through continuous monitoring.

3. Scope

This policy applies to all CCTV systems operated on Brunel University London premises (including buildings, grounds, car parks, and other facilities) and to mobile equipment such as drones/UAVs and Body Worn Video (BWV).

4. Principles

- 4.1 CCTV surveillance shall comply with all relevant legislation, including the Data Protection Act, Human Rights Act, UK GDPR, and Martyn's Law.
- 4.2 CCTV systems shall only be used for crime prevention, public safety, and the protection of property and assets.
- 4.3 The use of CCTV shall be proportionate to identified risks and shall not be excessive.
- 4.4 Prominent signage shall indicate the presence of CCTV surveillance in covered areas.
- 4.5 Access to CCTV footage shall be restricted to authorised personnel on a need-to-know basis (e.g., Community Policing and Security, law enforcement, and university management for HR investigations).
- 4.6 No CCTV installation may be deployed on University property (including managed property) without prior approval from the Community Policing and Security Department, including a Security Vulnerability Assessment and Operational Requirement. Unauthorised cameras will be removed.

5. Body Worn Video (BWV)

5.1 Purpose BWV may be used by the Community Policing and Security Department to record incidents, interactions, and activities for security and safety purposes.

5.2 Operational Guidelines

- BWV shall only be activated where there is a legitimate operational need (e.g., responding to incidents or collecting evidence, including first accounts).
- BWV recordings shall follow the same principles of lawfulness, purpose limitation, proportionality, transparency, and access control as fixed CCTV systems.
- Personnel using BWV shall receive appropriate training on its use, privacy considerations, and data protection requirements.

6. Responsibilities

6.1 Head of Security and Emergency Planning

- Ensure overall compliance with this policy and relevant legislation.
- Allocate resources for installation, maintenance, and operation of CCTV systems.
- Work with the Data Protection Officer on compliance and disclosure requests.

6.2 Community Policing and Security Department – Control Room

- Operate and manage CCTV and BWV systems in accordance with this policy.
- Review footage for security incidents.
- Maintain records of operations, including retention and access logs.

6.3 Staff and Users

- Comply with this policy and any related instructions.
- Report concerns or incidents to the Community Policing and Security Department.

7. Access and Retention

- Access to footage is restricted to authorised personnel on a need-to-know basis.
- Footage shall normally be retained for a maximum of 31 days, in line with legal requirements and operational needs. Longer retention may apply where footage is relevant to an ongoing incident or investigation.

8. Review and Compliance

This policy shall be reviewed periodically (at least annually) to ensure its continued effectiveness and compliance with evolving legal and operational requirements. Updates will be communicated to relevant stakeholders.

9. Covert Surveillance

Covert surveillance (monitoring or recording without the knowledge or consent of those affected) requires careful justification and strict oversight.

- 9.1 All covert surveillance must be approved by the Chief Operating Officer and the Data Protection Team, upon request by the Head of Security and Emergency Planning. A detailed justification and privacy impact assessment are required.
- 9.2 Operations must comply with the Regulation of Investigatory Powers Act (RIPA), Investigatory Powers Act (IPA), and all other relevant legislation.
- 9.3 Data must be handled in accordance with UK GDPR, with appropriate safeguards.
- Records of all covert operations shall be maintained and subject to review by the Data Protection Team.

10. Security and Cyber Security of CCTV Systems

The University recognises that CCTV systems process and store personal data and form part of its information technology infrastructure. Therefore, CCTV systems shall be managed as secure information systems as well as surveillance systems.

Appropriate technical and organisational measures shall be implemented to protect CCTV networks, cameras, recording devices, management platforms, user accounts, and recorded footage from unauthorised access, compromise, alteration, loss, or disclosure.

CCTV systems shall operate in accordance with the University's Information Security Management System (ISMS) and associated information security policies, standards, and procedures. As a minimum, the following controls shall be applied:

- Access shall be restricted to authorised personnel with explicit approval from the Head of Security and Emergency Planning.
- All access and activity shall be subject to audit logging.
- Systems shall be securely configured and maintained, including timely patch management by authorised contractors and Information Services.
- Remote access arrangements (including for support providers) shall be appropriately secured and controlled.
- Stored and exported footage shall be protected against unauthorised access, alteration, loss, or disclosure.
- Information security requirements shall be considered throughout the full lifecycle of CCTV systems.

Disclaimer

The operation of CCTV on University premises is conducted solely to enhance safety and security. There is no legal obligation to operate CCTV systems. While every effort is made to protect privacy, footage may be used for legitimate investigative purposes in accordance with applicable laws. Enquiries should be directed to the Community Policing and Security Department.