Brunel University CCTV

March, 2024

V1

	CHANGE LOG	
03/2024	V1 New current policy	Terry Vass
09/2024	Policy was approved at IAC	Terry Vass

CCTV – Control Room

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 including 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 multifaceted, aligning with BUL's commitment to safety and security. These objectives include:

- Protection of Stakeholders and Assets: Safeguarding the well-being of our staff, students, visitors, and the valuable assets of the BUL community is our top priority.

- Crime Prevention and Detection: Our CCTV system plays a crucial role in deterring criminal activities, as well as investigating and detecting disciplinary offenses in strict accordance with University disciplinary procedures.

- Apprehension and Prosecution of Offenders: We leverage the power of CCTV images and data to support the apprehension and prosecution of offenders. This includes utilising captured visuals as evidence in both criminal and civil proceedings.

- Premises Security Monitoring: The continuous monitoring of our premises enhances overall security, allowing for timely responses to potential threats or incidents.

3. **Scope**

This policy applies to all CCTV systems operated within Brunel University London premises, including but not limited to buildings, grounds, car parks, and other facilities.

This policy applies to all CCTV systems operated within Brunel University London premises, including but not limited to buildings, grounds, car parks (including ANPR), and other facilities, as well as mobile equipment such Drones/UAVs and BWV.

4. **Principles**

4.1. CCTV surveillance shall be conducted in compliance with all relevant legislation, including but not limited to the Data Protection Act, Human Rights Act, and General Data Protection Regulation (GDPR).

4.2. CCTV systems shall only be used for the purposes of crime prevention, public safety, and the protection of property and assets.

4.3. The use of CCTV shall be proportionate to the identified security and safety risks and shall not be excessive in nature.

4.4. Signs indicating the presence of CCTV surveillance shall be prominently displayed in areas covered by CCTV cameras.

4.5. Access to CCTV footage shall be restricted to authorised personnel on a need to know basis, such as Community Policing and Security, law enforcement agencies, and university management as per HR policy on investigations.

4.6. No CCTV installation is to take place on Brunel University Property (inc managed property) without the Community Policing and Security Department's knowledge, Security Vulnerability Assessment and Operation Requirement. Any unauthorised CCTV cameras found will be removed.

5. **Body Worn Video (BWV)**

5.1. Purpose: Body Worn Video (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 in situations where there is a legitimate reason for its use, such as responding to incidents or for the exhibiting, recording of evidence, including first accounts.
- BWV recordings shall adhere to the same principles of lawfulness, purpose limitation, proportionality, transparency, and access control as outlined for CCTV systems.
- Personnel equipped with BWV shall undergo appropriate training on its use, including privacy considerations and data protection requirements.

6. **Responsibilities**

6.1. Head of Security and Emergency Planning:

- Ensure compliance with this CCTV policy and relevant legislation.
- Allocate resources for the installation, maintenance, and operation of CCTV systems.
- Work with the Data Protection Officer (DPO) to ensure compliance with data protection laws, as well as discuss disclosure requests.

6.2. Community Policing and Security Department – Control Room:

- Operate and manage CCTV systems and BWV equipment in accordance with this policy.
- Conduct regular reviews of CCTV footage to detect and investigate security incidents.
- Maintain records of CCTV operations, including footage retention and access logs in the **Book 105**.

6.3. Staff and Users:

- Adhere to this policy and follow any instructions provided regarding CCTV and BWV usage.
- Report any concerns or incidents related to CCTV surveillance to the Community Policing and Security Department.

7. **Access and Retention**

7.1. Access to CCTV footage shall be restricted to authorised personnel on a need to know basis, such as Community Policing and Security, law enforcement agencies, and university management as per HR policy on investigations.

7.2. CCTV footage shall be retained for 31 days +/- in accordance with legal requirements and operational needs. However, specific retention periods shall be determined based on factors such as the nature of the footage and its relevance to security or safety incidents.

8. **Review and Compliance**

This CCTV policy shall be periodically reviewed to ensure its effectiveness and compliance with evolving legal and operational requirements. Any updates or revisions shall be communicated to relevant stakeholders.

9. **Covert Surveillance**

Covert surveillance refers to the monitoring or recording of individuals or activities without their knowledge or consent. Brunel University London recognises that the use of covert surveillance requires careful consideration and must be conducted in accordance with legal and ethical standards.

9.1. The use of covert surveillance must be approved by both the Chief Operating Officer and the Data Protection Team and requested by the Head of Security and Emergency Planning.

A detailed justification for the need for covert surveillance must be provided, outlining the specific risks or concerns that cannot be addressed through other means.

Any proposed covert surveillance operation must undergo a thorough risk assessment, including an evaluation of the potential impact on individuals' privacy rights.

9.2. Covert surveillance operations must comply with all relevant legislation, including the Regulation of Investigatory Powers Act (RIPA) and the Investigatory Powers Act (IPA).

The necessity and proportionality of covert surveillance must be carefully assessed, taking into account the rights and freedoms of individuals.

9.3. Data collected through covert surveillance must be handled in accordance with data protection laws, including the General Data Protection Regulation (GDPR).

Adequate safeguards must be implemented to protect the security and confidentiality of the surveillance data.

9.4. The use of covert surveillance must be conducted with transparency and accountability.

Records of covert surveillance operations, including the rationale for their use and any outcomes, must be maintained and made available for review upon request.

9.5. Covert surveillance operations shall be subject to regular review and oversight by the Data Protection Team to ensure compliance with legal and ethical standards.

Any concerns or complaints regarding the use of covert surveillance shall be promptly investigated and addressed.

9.6. Personnel involved in the planning and execution of covert surveillance operations must receive appropriate training on the legal and ethical considerations involved.

Disclaimer:

Please be advised that the operation of Closed-Circuit Television (CCTV) on our premises is conducted solely for the benefit of enhancing safety and security for campus users. It is important to note that there exists no legal requirement mandating our institution to operate CCTV surveillance systems. We emphasise that the deployment of CCTV cameras is solely a proactive measure to safeguard the well-being of individuals within our campus environment. Additionally, while every effort is made to ensure the protection of privacy rights, it should be understood that CCTV footage may be utilised for investigative purposes in accordance with applicable laws and regulations. Users of our facilities are encouraged to familiarise themselves with our policies regarding CCTV surveillance. Should you have any inquiries or concerns regarding our CCTV operations, please do not hesitate to contact the Community Policing and Security Department.