

CCTV Policy

Index

<u>1.</u>	<u>Introduction</u>	<u>4</u>
<u>2.</u>	<u>Compliance</u>	<u>4</u>
<u>3.</u>	<u>Purpose</u>	<u>4</u>
<u>4.</u>	<u>Description</u>	<u>5</u>
<u>5.</u>	<u>Operation</u>	<u>5</u>
<u>6.</u>	<u>Information retention</u>	<u>5</u>
<u>7.</u>	<u>Access</u>	<u>5</u>
<u>8.</u>	<u>Related regulations, policies, and procedures</u>	<u>6</u>
<u>9.</u>	<u>Contact Us</u>	<u>6</u>
<u>10.</u>	<u>Review</u>	<u>6</u>

Document Version Control

Committee	Committee Action	Date
SMT	Approved	03 July 2024
	Date in force	22 July 2024
N/A	Reviewed by S Middleton (Next review in the next Academic Year.)	03 February 2025
	Date in force	05 February 2025
N/A	Reviewed by S Middleton (Next review in the next Academic Year.)	12 January 2026
	Date in force	14 January 2026

The CCTV Policy will be reviewed annually by the Document Lead. Any significant changes beyond the scope of an annual review will require the approval of the Senior Management Team (SMT).

1. Introduction

Bloomsbury Institute ("the Institute") operates a CCTV surveillance system ("the system") throughout its premises, with images being monitored and recorded on each site. The system is owned and managed by the Institute and operated by the Estates and Facilities Department with first level technical and networking support provided by the IT Services Department.

2. Compliance

Images obtained from the system (which include recognisable individuals) constitute personal data and are covered by the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR). This Policy should therefore be read in conjunction with the Institute's [Data Protection and Confidentiality Policy](#), [Privacy Notice](#), [Freedom of Information Policy](#)¹, the [Data Protection Act \(2018\) Code of Practice](#)² and the UK GDPR)³.

Bloomsbury Institute is the registered Data Controller under the terms of the Data Protection Act 2018. The Data Protection Officer for the Institute is the Head of Compliance (dpo@bil.ac.uk), who is responsible for ensuring compliance with the Act.

This policy has been drawn up in accordance with the advisory guidance contained within the Information Commissioner's [Guidance on Video Surveillance](#)⁴ and the [Home Office Surveillance Camera Code of Practice](#)⁵.

3. Purpose

The Institute's registered purposes for processing personal data through use of the system are security, safety and crime prevention. These purposes are further defined as:

- CCTV is used for maintaining public safety, the security of property and premises and for preventing and investigating crime. It may also be used to monitor staff when carrying out work duties. For these reasons, the information processed may include visual images, personal appearance and behaviours. This information may be about staff, customers and clients, members of the public and those inside or entering the building, or in the immediate vicinity of the area under surveillance.
- Where necessary or required, this information will be shared with the data subjects themselves, employees and agents, service providers, police forces, court or tribunal, security organisations and any qualified persons making an enquiry.

The operators of the system receive training which includes the impact of such systems on individuals and their right to privacy. All staff are made aware of and required to follow the Institute's Privacy Notice and Data Protection Policy.

Full details of the Institute's data protection registration are available on the [Information Commissioner's Office website](#)⁶.

¹ These policies can be found at <https://www.bil.ac.uk/qem/policies/>.

² <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

³ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

⁴ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/>

⁵ https://assets.publishing.service.gov.uk/media/619b7b50e90e07044a559c9b/Surveillance_Camera_CoP_Accessible_PDF.pdf

⁶ <https://ico.org.uk/>

4. Description

The system is intended to produce images that are as clear as possible and appropriate for the purposes stated. The system is operated to provide (when required) information and images of evidential value.

Cameras may be located at strategic points throughout the Institute's estate, principally at the entrance and exit points of buildings, in rooms with high value contents (e.g., the Digital Studio and Server Rooms), and main thoroughfares.

A secondary CCTV system is installed to cover the Bloomsbury Radio studio.

Signage is prominently placed at strategic points on the estate to inform staff, students, and visitors that CCTV is in use.

5. Operation

Images captured by the system are recorded continuously and may be monitored by staff who are trained and designated as CCTV Operators. Images displayed on monitors are not visible from public areas and access to the system is strictly limited. Although the system installed can record sound, we do not record sound and staff are unable to listen to conversations.

Staff working with the system are made aware of the sensitivity of handling CCTV images and recordings. They are fully briefed and trained in all aspects of the operational and administrative functions of the system and must complete mandatory GDPR training.

IT Services are classified as operators when they are needed to resolve connectivity issues. They are not permitted to perform any surveillance or data gathering tasks and are deployed only to maintain the system.

6. Information retention

Images and information are not stored longer than is required for the stated purpose. Images are deleted once their purpose has been fulfilled. Images and footage will be overwritten on a 30-day rolling basis. The secondary CCTV system in the Bloomsbury Radio studio runs on a 14-day rolling basis.

Information used as a reference database, such as still images captured by the automated system, are kept until such time as they become unnecessary. At this point, they are deleted.

In the case of events of interest, which may include, but are not limited to, proof of theft or proof of violence, the images will be stored until such time as they are no longer required.

7. Access

Access to recorded images is restricted to those who need to have access in accordance with this policy, the Institute's [Data Protection and Confidentiality Policy](#), [Privacy Notice](#), [Freedom of Information Policy](#)⁷, the Standard Operating Procedures ("SOPs") and any governing legislation. The main users and operators of the system are the Estates and Facilities team and the IT Services team.

Disclosure of recorded material will only be made to third parties in accordance with the purposes of the system and in compliance with the Data Protection Act 2018.

⁷ These policies can be found at <https://www.bil.ac.uk/qem/policies/>

CCTV Footage Requests should be addressed to dpo@bil.ac.uk using the [CCTV Footage Request Form](#)⁸

8. Related regulations, policies, and procedures

External

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- A data protection code of practice for surveillance cameras and personal information
- Surveillance camera code of practice

Internal

- Data Protection and Confidentiality Policy
- Privacy Notice
- Freedom of Information Policy

9. Contact Us

Students and visitors should address any concerns, complaints, or queries over the use of the Institute's CCTV system to:

Email: estates.facilities@bil.ac.uk

Telephone: +44 (0) 20 7078 8840

Post: Estates and Facilities Manager, Bloomsbury Institute, 7 Bedford Square, London WC1B 3RA

10. Review

This policy is reviewed annually by the Document Lead. Any significant changes beyond the scope of an annual review will require the approval of the Senior Management Team (SMT).

⁸

<https://bloomsburyinstitute.sharepoint.com/:w/s/EstatesFacilities2/IQBEsnhnE1aBQLyhQbjhoPDcAcVjITnYpY3FDrKStP5r1oY?e=ggrKCq>