

CLOSED CIRCUIT TELEVISION (CCTV) POLICY

V1.0

Policies superseded by this version

This document replaces the 2 individual existing CCTV policies from legacy City and St Georges organisations.

Summary of changes to previous version

This policy has been reviewed and restructured in accordance with the City St George's Policy Template Version 3.

The policy has not materially changed the operational purpose of the University's CCTV systems but has been reformatted to separate governance requirements from operational procedures. Existing responsibilities, legislative requirements and operational controls have been consolidated to improve clarity and support consistent implementation across all campuses.

Table of contents

Section:	Heading:	Page number:
1	Introduction	1
2	Freedom of Speech and Academic Freedom	2
3	Equity, Diversity and Inclusion	2
4	Definitions	2
5	Policy	3
6	Procedure	6
7	Advice and guidance	10
8	Failure to comply	10
9	Review	11
Appendix A	Surveillance Camera Code Principles	13

1 Introduction

1.1 Purpose

City St George's, University of London is committed to providing a safe, secure and welcoming environment for students, staff, contractors, visitors and members of the public using its campuses.

The University recognises that Closed Circuit Television (CCTV) forms an important component of its wider physical security strategy and provides an effective means of supporting the prevention and detection of crime, reducing anti-social behaviour, protecting University assets, supporting investigations, safeguarding individuals and assisting emergency response.

The University operates CCTV systems only where there is a legitimate operational need and where their use is lawful, necessary and proportionate. CCTV is not intended to replace good physical security, appropriate staffing levels or effective management controls but forms part of an integrated security strategy.

This policy establishes the governance framework for the operation, management and use of CCTV systems throughout the University and explains the standards expected of everyone involved in their operation.

The policy also demonstrates the University's commitment to protecting the privacy and rights of individuals whilst ensuring that CCTV systems remain an effective security measure.

1.2 Legislative Context

Legislation compliance requirements are set out in section 5.4 of this policy

1.3 Objectives

The objectives of the University's CCTV systems are to:

- Assist in preventing crime and disorder;
- Deter anti-social behaviour;
- Improve the safety and wellbeing of staff, students, contractors and visitors;
- Protect University buildings, equipment and assets;
- Support investigations into criminal, disciplinary and safeguarding matters;
- Provide evidential material where appropriate;
- Assist emergency services during incidents;
- Support the effective management of University premises.

The University will ensure that CCTV is used solely for legitimate operational purposes and not for monitoring staff or students without lawful justification.

2 Freedom of Speech and Academic Freedom

- 2.1 City St George's, University of London, regards freedom of speech and academic freedom to be fundamental to delivering its mission as the University of business, practice and the professions. Its values in this respect are set out in a code of practice on freedom of speech and academic freedom, which explains how the University will uphold, secure, and promote freedom of speech within the law: <https://www.citystgeorges.ac.uk/about/governance/policies/code-of-practice-on-freedom-of-speech>.

Nothing in this policy should be interpreted in any way that would be inconsistent with the code of practice and – in the event of any inconsistency – the provisions of the code will prevail.

3 Equity, Diversity and Inclusion

- 3.1 City St George's, University of London works to advance equity, diversity and inclusion in its activities, processes, and culture, for the whole University community, including staff, students and visitors.

The University will meet its obligations under the Equality Act 2010 in its policies and seek to eliminate discrimination on the basis of age, caring responsibilities, disability, gender identity, gender reassignment, marital status, neurodiversity, pregnancy, race, religion or belief, sex, sexual orientation, and socio-economic background.

4 Definitions

- 4.1 **Authorised Person** - An employee, contractor or appointed person acting on behalf of City St George's, University of London, who has been formally authorised to access CCTV systems or recorded footage in connection with their duties.
- 4.2 **Body Worn Video (BWV)** - A wearable camera used by Security personnel to record incidents where footage may be required for evidential, safety, welfare or investigative purposes.

- 4.3 **CCTV** - Closed Circuit Television systems operated by the University for the purposes described within this policy.
- 4.4 **Recorded image** – Any still image, video footage or digital recording captured by a University CCTV or body worn video system regardless of storage location.
- 4.5 **Data Controller** - City St George's, University of London, acting as the organisation responsible for determining the purposes and means of processing personal data captured by CCTV systems.
- 4.6 **Personal Data** - Any information relating to an identified or identifiable individual, including recorded CCTV images.
- 4.7 **Subject Access Request (SAR)** - A request made by an individual seeking access to personal data held about them under applicable data protection legislation.
- 4.8 **Data Protection Impact Assessment (DPIA)** – A documented assessment undertaken to identify and mitigate privacy risks associated with the installation, modification or operation of CCTV systems/

5 Policy

5.1 Scope

This policy applies to all CCTV systems owned, managed or operated by City St George's, University of London.

The policy applies to:

- Fixed CCTV cameras.
- Pan, Tilt and Zoom (PTZ) cameras.
- Digital recording equipment.
- CCTV management software.
- Network infrastructure supporting CCTV systems.
- Body Worn Video cameras issued to Security personnel.
- Associated image storage and retrieval systems.

This policy applies to all members of staff, students, contractors, consultants and third parties who are responsible for managing, operating, maintaining or accessing CCTV systems on behalf of the University.

The policy applies across all University campuses where CCTV systems are operated by the University.

The policy does not apply to audio-visual recording systems installed solely for teaching, learning, conferencing or lecture capture purposes where separate governance arrangements exist.

5.2 Principles

The University is committed to ensuring that CCTV systems are operated responsibly and in accordance with recognised good practice.

The following principles shall apply throughout the operation of all CCTV systems.

Lawfulness

CCTV shall only be used where there is a lawful basis for processing personal data and where the use of surveillance is necessary to achieve a legitimate operational objective.

Necessity and Proportionality

CCTV systems shall only be installed where less intrusive measures would not provide an appropriate level of protection.

Camera locations, recording capability and retention periods shall remain proportionate to the risks being managed.

Transparency

The University will ensure that individuals are informed where CCTV is in operation through appropriate signage, privacy information and published guidance.

Privacy

Every effort shall be made to minimise unnecessary intrusion into private areas.

Cameras shall not intentionally monitor areas where individuals have a reasonable expectation of privacy, including toilets, changing facilities or shower areas.

Security

Recorded images shall be protected against unauthorised access, alteration, disclosure or loss through appropriate technical and organisational controls.

Accountability

The University shall maintain appropriate governance arrangements to demonstrate compliance with data protection legislation and shall regularly review the operation of CCTV systems.

5.3 Roles and Responsibilities

Head of Security

The Head of Security is responsible for the operational management of the CCTV system and shall:

- Ensure CCTV systems operate in accordance with this policy;
- Authorise operational procedures;
- Ensure appropriate staff training is delivered;
- Oversee compliance monitoring and annual policy reviews;
- Authorise retention of images beyond normal retention periods where operationally justified;
- Approve operational changes to CCTV systems;
- Ensure appropriate audit arrangements are maintained.

Information Technology Services

Information Technology Services shall support the resilience, availability and security of CCTV infrastructure including servers, storage, networking and software platforms.

They shall work in partnership with Security to maintain system integrity and ensure appropriate cyber security controls are implemented.

Information Assurance Team

The Information Assurance Team shall provide specialist advice relating to:

- UK GDPR compliance;
- Data Protection Act 2018;
- Subject Access Requests;
- Requests for disclosure;
- Data Protection Impact Assessments;
- privacy considerations associated with CCTV systems.

Security Staff

Authorised Security personnel shall:

- Operate CCTV systems only for legitimate operational purposes;
- Maintain confidentiality of recorded images;
- Comply with all operating procedures;
- Report faults or suspected misuse immediately;
- Complete mandatory training before being granted access to CCTV systems.

Managers

Managers responsible for areas protected by CCTV shall consult the Head of Security before requesting:

- New CCTV installations;
- Relocation of cameras;
- Removal of cameras;
- Significant operational changes.

5.4 Legislative and Regulatory Compliance

The University shall operate all CCTV systems in accordance with applicable legislation and recognised good practice, including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Human Rights Act 1998;
- Protection of Freedoms Act 2012;
- Freedom of Information Act 2000;
- Information Commissioner's Office guidance relating to video surveillance;
- BS 7958:2015 Closed Circuit Television (CCTV) Management and Operation;
- Surveillance Camera Code of Practice.

Where legislation, statutory guidance or recognised good practice changes, the University will review this policy and associated procedures to ensure continued compliance.

5.5 Governance, Monitoring and Assurance

The University will maintain governance arrangements to ensure CCTV systems continue to operate effectively, proportionately and in accordance with this policy.

This will include:

- Regular operational reviews of CCTV systems;
- Periodic review of camera locations and coverage;
- Monitoring compliance with retention and disclosure requirements;
- Maintenance of appropriate audit trails;
- Completion and review of Data Protection Impact Assessments where required;
- Annual reporting on the operation and effectiveness of the CCTV system;
- Review of this policy at least every twelve months or sooner where legislative or operational changes require.

The Head of Security shall ensure that any recommendations arising from audits, inspections, incident investigations or changes in legislation are incorporated into future revisions of this policy and associated operational procedures.

6 Procedure

6.1 CCTV System Overview

The University operates integrated digital CCTV systems across its campuses to support the delivery of a safe, secure and resilient environment for staff, students, contractors and visitors.

The systems are designed to support the prevention and detection of crime, assist in the investigation of incidents, protect University property and assets, provide evidential material where appropriate, and support the effective management of security incidents.

At the time of publication, the University operates the Genetec Security Center platform across the Clerkenwell and Moorgate campuses and the Pelco VideoXpert (VX Ops Centre) platform at the Tooting campus. These systems provide authorised Security personnel with live monitoring, alarm management, playback of recorded footage, evidential retrieval and reporting functionality.

The University's CCTV platforms may be upgraded, replaced or enhanced as operational requirements change. Such changes shall not require amendment to this policy provided the operational principles, governance arrangements and legislative requirements contained within this document continue to be met.

Body Worn Video (BWV) devices may also be issued to authorised Security personnel. These cameras are overt recording devices and will normally only be activated where an incident is occurring, where there is an identified risk to the safety of staff or others, or where the recording of evidence is considered necessary and proportionate.

Recordings obtained through Body Worn Video systems shall be managed in accordance with the same legislative requirements, governance arrangements, retention periods and disclosure processes that apply to fixed CCTV systems.

Changes to CCTV infrastructure, including the installation of new cameras, relocation of existing cameras, changes in recording capability or significant alterations to system configuration, shall be

subject to an operational assessment and, where appropriate, review of the University's Data Protection Impact Assessment (DPIA) before implementation.

6.2 CCTV Operation

CCTV systems operate continuously to provide an appropriate level of security monitoring across the University's campuses.

Images are recorded digitally using secure on-site servers located within protected data centre environments. Access to recording equipment and associated infrastructure is restricted to authorised personnel.

The University's CCTV systems are configured to provide images of sufficient quality to enable the systems to fulfil their intended operational purposes.

Security personnel shall undertake routine checks to ensure that:

- Cameras remain operational;
- Image quality remains suitable for evidential purposes;
- Recording equipment is functioning correctly;
- Camera views remain appropriate;
- Date and time settings remain accurate.

Where faults are identified, these shall be reported promptly through the University's maintenance arrangements to minimise disruption to security operations.

All recorded images remain the property of City St George's, University of London.

6.3 Access to and Viewing of CCTV Images

Live and recorded CCTV images shall only be viewed by authorised persons where there is a legitimate operational requirement.

- Authorised viewing facilities are currently located within:
- The Security Control Room, Northampton Square;
- The Security Office, Bunhill Row;
- The Hunter Wing Security Control Room, Tooting;
- Horton Halls Reception.

Additional authorised viewing locations may be approved by the Head of Security where operational requirements justify such access.

For the purposes of this policy, an authorised person is an employee or appointed individual acting on behalf of the University who has a legitimate operational requirement to access CCTV images in connection with the prevention or detection of crime, safeguarding, security management or the investigation of incidents.

Individuals involved in formal disciplinary investigations may also be granted access where authorised by the Head of Security and where such access is necessary to support the investigation.

CCTV images shall not be viewed in the presence of unauthorised persons.

Where CCTV software is accessed via desktop workstations, screens shall be locked or minimised whenever they are unattended or where recorded images could be viewed by persons who are not authorised.

Access permissions shall be reviewed periodically to ensure that only those with a continuing operational requirement retain access to CCTV systems.

6.4 Processing and Retention of CCTV Images

The processing of CCTV images shall be undertaken in accordance with UK GDPR, the Data Protection Act 2018 and this policy.

Recorded images shall only be processed for legitimate operational purposes including:

- Prevention and detection of crime;
- Investigation of security incidents;
- Safeguarding;
- Protection of individuals;
- Protection of University property and assets;
- Disciplinary investigations where appropriate;
- Compliance with legal obligations.

CCTV cameras shall not intentionally capture images from areas where individuals have a reasonable expectation of privacy, including toilets, shower facilities or changing rooms.

Recorded footage shall normally be retained for a maximum period of 30 days, after which it will be automatically overwritten through the normal operation of the recording system.

Where recorded images are required for:

- Criminal investigations;
- Disciplinary proceedings;
- Safeguarding investigations;
- Civil proceedings;
- Insurance claims;
- Statutory investigations;
- Any other lawful purpose,

The Head of Security, or an authorised deputy, may approve retention beyond the standard retention period.

Images retained beyond thirty days shall be securely stored with access restricted to authorised personnel and shall be reviewed periodically to ensure continued retention remains necessary and proportionate.

Once the lawful purpose for retention no longer exists, the recorded images shall be securely and permanently deleted.

6.5 Requests for CCTV Images

Requests for access to CCTV footage shall be submitted using the University's approved request process. The requester should email cctv@citystgeorges.ac.uk in the first instance.

Requests shall contain sufficient information to enable the relevant images to be identified, including the location, date, time and nature of the incident. All requests shall be assessed by the Head of

Security, or an authorised delegate, to determine whether disclosure is lawful, necessary and proportionate.

Where a request raises data protection considerations or involves the disclosure of personal data, advice shall be sought from the Information Assurance Team before disclosure is authorised.

The University shall maintain a record of all requests received, decisions made and disclosures completed.

6.6 Disclosure to Law Enforcement Agencies

Requests from law enforcement agencies shall be considered in accordance with applicable legislation.

Where disclosure is approved, the University shall satisfy itself that:

- The request has been made by an authorised investigating officer;
- Disclosure is necessary for the prevention or detection of crime or another lawful purpose;
- An appropriate legal basis exists for disclosure.

The University shall maintain a record of all disclosures including:

- The requesting organisation;
- The identity of the requesting officer;
- The purpose of the request;
- The incident or crime reference number, where applicable;
- The date of disclosure;
- The method used to transfer the recorded images.

Recorded images shall be transferred using secure methods appropriate to the sensitivity of the information being disclosed.

Where there is an urgency for relevant information to be shared ie. The police have a suspect in custody and such information is integral to charging or an incident has occurred that is otherwise linked to public safety, the Head of Security may authorise the immediate release of footage on the expectation that an official request is made as soon as reasonably practicable. The security team will document this accordingly.

6.7 Data Protection and Information Governance

The University shall ensure that all processing of CCTV images complies with applicable data protection legislation.

Appropriate technical and organisational measures shall be implemented to protect recorded images against unauthorised access, disclosure, alteration or loss.

All staff authorised to access CCTV systems shall receive appropriate training in the operation of the system and the requirements of data protection legislation before access is granted.

Data Protection Impact Assessments shall be completed where required and reviewed whenever significant changes are made to the University's CCTV systems.

6.8 Monitoring, Audit and Review

The operation of the CCTV system shall be subject to ongoing monitoring and periodic audit.

The Head of Security shall produce an annual review of the operation of the University's CCTV systems, including compliance with this policy, legislative requirements, operational effectiveness and recommendations for improvement.

Findings from audits, inspections, incident investigations and legislative changes shall be incorporated into future revisions of this policy and associated operational procedures.

6.9 Complaints

Any individual wishing to raise a concern regarding the operation of the University's CCTV systems may do so through the University's complaints procedures.

Complaints relating to the processing of personal data or the operation of CCTV shall be investigated by the appropriate University department and responded to in accordance with the University's complaints procedures and applicable data protection legislation.

Where an individual remains dissatisfied following completion of the University's internal processes, they may refer the matter to the Information Commissioner's Office.

7 Advice and guidance

The University recognises that the effective operation of CCTV systems depends upon staff understanding both their operational responsibilities and the legal framework governing the use of surveillance systems.

Advice regarding the interpretation or implementation of this policy should be sought before any action is taken that may affect the operation of the University's CCTV systems.

Operational advice relating to CCTV installations, system operation, access to recorded images, Body Worn Video, evidential requirements or security investigations should be obtained from the Head of Security or an authorised member of the Security Management Team.

Advice relating to data protection, privacy, Subject Access Requests (SARs), Freedom of Information requests, disclosure of recorded images or compliance with UK GDPR should be obtained from the Information Assurance Team.

Requests for CCTV footage should be submitted through the University's approved request process. Requests should include sufficient information to enable the relevant images to be identified, including the location, date, approximate time and nature of the incident.

Where appropriate, requests will be reviewed jointly by the Head of Security and the Information Assurance Team to ensure that any disclosure of personal data is lawful, necessary and proportionate.

Where uncertainty exists regarding the operation of this policy or the lawful processing of recorded images, advice should always be sought before any disclosure or use of CCTV footage is authorised.

8 Failure to comply

The University regards the misuse of CCTV systems or recorded images as a serious matter.

Failure to comply with this policy, associated procedures or applicable legislation may result in disciplinary action under the University's relevant staff or student procedures.

Examples of non-compliance include, but are not limited to:

- Accessing CCTV systems without appropriate authorisation;
- Viewing recorded images without a legitimate operational reason;
- Disclosing CCTV images without appropriate authority;
- Copying or retaining recorded images outside approved University systems;
- Using CCTV systems for personal purposes;
- Interfering with or deliberately damaging CCTV equipment;
- Failing to comply with data protection legislation or this policy.

Where appropriate, breaches of this policy may also result in:

- Withdrawal of access to CCTV systems;
- Internal investigation;
- Referral to the Information Commissioner's Office;
- Referral to the Police or other law enforcement agencies;
- Civil or criminal proceedings where legislation has been breached.

Contractors or third parties who fail to comply with this policy may have their access to University premises withdrawn and may be subject to contractual remedies in addition to any legal action.

9 Review

This policy shall be reviewed every twelve months or sooner where required by:

- Changes to legislation or statutory guidance;
- Changes to University governance arrangements;
- Significant changes to CCTV technology or operational practice;
- Recommendations arising from audits or inspections;
- Findings from investigations into security incidents;
- Organisational changes affecting the management of CCTV.

Responsibility for reviewing this policy rests with the Head of Security.

The policy shall be approved in accordance with the University's Policy Framework and Governance arrangements.

The effectiveness of this policy shall be monitored through:

- Annual operational reviews;
- Periodic compliance audits;
- Data Protection Impact Assessments;
- Internal and external audit findings;
- Analysis of security incidents involving CCTV;
- Feedback from stakeholders and operational users.

Policy information

Should you require further information regarding this policy or access to the policy in an alternative format, then please contact Chris Saich, Head of Security.

Policy Title:	Closed Circuit Television (CCTV) Policy
Policy Version:	V1.0
Primary Author:	Chris Saich, Head of Security
Related Policies:	Security Policy Data Protection Policy Information Security Policy Records Management Policy Physical Security Standards Visitor Management Policy
Accountable Authority:	Velda Ismay, Assistant Director, Facilities Management
Approving Authority:	Information Governance Committee
Date of Approval:	TBC
Policy effective from:	TBC
Date of Review:	12 months from approval

Appendix

Appendix A – Surveillance Camera Code Principles

The University adopts the principles contained within the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012.

These principles underpin the operation of the University's CCTV systems and shall be considered whenever CCTV systems are installed, reviewed or modified.

The twelve guiding principles are:

- Use of surveillance shall always be for a specified purpose that is necessary to meet an identified pressing need.
- The use of CCTV shall take account of its effect on individuals and their privacy.
- Responsibility and accountability for surveillance systems shall be clearly defined.
- Clear rules, policies and procedures shall govern the operation and use of CCTV.
- Appropriate safeguards shall exist in relation to access to and disclosure of recorded images.
- Recorded images shall be retained only for as long as necessary.
- Access to recorded images shall be restricted to authorised persons.
- All operators shall receive appropriate training.
- Security measures shall protect CCTV systems against misuse.
- CCTV systems shall be used effectively and support their intended operational purpose.
- Appropriate review and audit arrangements shall be maintained.
- The continued use of CCTV shall remain justified, proportionate and subject to regular review.