Closed Circuit Television (CCTV) POLICY

Maintained by:	Department of Estates, Environment and Facilities
Owned by:	Department of Estates, Environment and Facilities
Last updated:	17th of December 2024
Date of next review:	January 2026
Current version:	v11.10

Contents

POLICY STATEMENT

City St George's, University of London, seeks to ensure as far as is reasonably practicable, the security, safety, welfare and wellbeing of all students, staff, visitors and contractors, whilst on University premises. To this end, CCTV camera recording devices are deployed within and around the estate to assist in the prevention, investigation and detection of crime; the control of anti-social behaviour; apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings); and the safety and welfare management of students, staff and visitors.

This Policy document summarises City St George's approach with respect to its Clerkenwell and Moorgate campuses, and should be read in conjunction with applicable privacy notices. Its aim is to explain how the approach is proportionate, lawful and compliant with relevant data protection, CCTV legislation and related guidance, including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act (DPA) 2018
- BS 7958-2015 CCTV Code of Practice
- ICO CCTV Code of Practice

1. Introduction

City St George's, University of London, is the owner of a CCTV Scheme which includes the recording of public areas and/or members of the public who may be visiting the premises. The University is a data controller in terms of the Data Protection Act 2018 and the UK GDPR. City St George's is registered with the Information Commissioner's Office (ICO) with the registration number **Z8947127**.

1.1 System Description

The system, Genetec, uses IP CCTV cameras.

Genetec is a unified open IP Security platform, which allows City St George's to manage CCTV, door controllers and other network infrastructure on its Clerkenwell and Moorgate campuses. These activities are consolidated under a single platform for real-time monitoring, reporting and playback. The platform allows unification of all data coming to and from the Security Operations Centre in the University Building. Adjustments are applied as necessary to support activities such as area refurbishments, change of use and new cameras. All adjustments are reviewed and approved by senior management.

1.2 Purpose of the System

The purpose of the CCTV system in use at City St George's is to enable the prevention, detection and investigation of crime and anti-social behaviour, and to monitor the security and safety of the premises and people on the premises.

City St George's CCTV system covers the Clerkenwell and Moorgate campuses at entrances/exits and main circulation areas (where appropriate e.g. areas accessed 24/7 or higher-risk and adjacent streets), to assist in the provision of a safe and secure environment for everyone on City St George's premises. CCTV aids the:

- prevention of crime and public disorder including anti-social behaviour;
- apprehension and prosecution of offenders in relation to the above;
- monitoring of public safety issues.

The University seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.

1.4 Operating Principles

The University will have due regard to the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although not a relevant authority, the University will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the Surveillance Camera Code of Practice principles. A summary of the principles is given at Annex I.

Personal data, including images recorded on the CCTV system, will be processed in line with the following principles:

- Fairly, transparently and lawfully processed;
- Processed for limited purposes and not further processed in a manner incompatible with those purposes;
- Adequate, relevant and not excessive in relation to the purposes for which they are processed;
- Accurate;
- Not kept for longer than is necessary for the purpose stated;
- Processed in accordance with individuals' rights;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. Operation

2.1 Scope

2.1.1 This Policy applies to all parts of the Clerkenwell and Moorgate University Estate with the exception of the leased premises, where CCTV systems and equipment may be operated and maintained locally by the landlord.

2.1.2 This Policy does not apply to the Webcam systems located in a number of meeting rooms and lecture theatres. These systems are used for educational purposes as part of City St George's AV system. The owners of these systems are responsible for ensuring appropriate signage is displayed in the areas of use explaining the purpose of their cameras and to distinguish them from those on the CCTV system.

2.1.3 Images are recorded centrally on servers located securely in the data center, as this service is hosted on the premises. Images are viewable in the Security Control Rooms by Security staff as appropriate.

2.1.4 The CCTV cameras provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are checked daily to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

2.1.5 All images recorded by the CCTV System remain the property and copyright of the University.

2.2 Responsibility

2.2.1 The Department of Estates, Environment and Facilities' Head of Security is responsible for the operation of City St George's CCTV system on the Clerkenwell and Moorgate campuses, which is supported by the IT Department.

2.2.2 Only the authorised EE&F/IT CCTV systems contractor(s) may be used in installing or maintaining CCTV systems associated with the University estate.

2.3 Viewing of CCTV images

2.3.1 The ability to view live and historical CCTV data available via network software will be made possible at the following locations by authorised persons only:

- The Security Control Room at Northampton Square;
- The Security Office at the Business School, Bunhill Row.

2.3.2 For the purpose of viewing CCTV images, an authorised person is defined as an employee or appointed person acting on behalf of City St George's, University of London, with a legitimate interest in the operational responsibility for prevention, investigation and detection of crime, as well as monitoring of security and safety, welfare and wellbeing at City St George's. Those involved in employee disciplinary processes may be authorised on a case-by-case basis.

2.3.3 Except where a request has been granted for third party access to certain specified recorded CCTV images (see below), CCTV images are not to be displayed in the presence of any unauthorised person or where such images may be inadvertently viewed by any unauthorised person. Where images are accessed or monitored on workstation desktops, the CCTV screen is to be minimised when not in use or unauthorised persons are present. Workstation screens must always be locked when unattended.

2.3.4 With the exception of the above, only members of the in-house security team or holders of a Security Industry Authority CCTV license, may view 'public space surveillance' CCTV footage as governed by the Private Security Industry Act 2001.

2.4 Processing CCTV Images:

2.4.1 It is imperative that access to, and security of, the images is managed in accordance with the requirements of the relevant legislation, manually indexed. At all times the following standards are to be applied:

2.4.2 Images must not be captured from areas in which individuals would have an expectation of privacy (i.e. toilets, changing facilities etc.).

2.4.3 CCTV images are recorded 24/7 and held in data storage. Images are not retained for longer than necessary. Data storage is automatically managed by the CCTV system software which is programmed to overwrite historical data in chronological order to enable the recycling of storage capabilities.

2.4.4 Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.

2.4.5 Where an image is required to be held in excess of the retention period referred to in the above, the Assistant Director of Facilities or the Head of Security (nominated deputy), will be responsible for authorising such a request.

2.4.6 Retained images are to be stored in a secure place which is access controlled. Images are to be permanently deleted when no longer required.

2.4.7 Images held in excess of their retention period will be reviewed on a three-monthly basis by the Assistant Director of Facilities or the Head of Security (nominated deputy). Any images that are not required for evidential purposes will be deleted.

2.4.8 Requests for CCTV images should be sent via email to cctv@city.ac.uk. This will generate a request via the IT ServiceNow portal. A reference number will be issued and the request will be handled by either the Security Department or the Information Assurance Team, as appropriate.

CCTV footage requests will be:

- Viewed as soon as possible after receipt
- Processed in accordance with urgency, priorities and statutory compliance deadlines .

There may be times when it is necessary to circumvent standard processes e.g. emergencies.

Once a decision has been reached in relation to the request, stakeholders will be notified and arrangements made accordingly for the sharing of the data with the requester, if that is the agreed outcome. This may differ depending on the type of request. The method for sharing the data will be agreed with the IT Information Security Manager.

2.5 Recorded Images

Cameras are sited to ensure that they cover University premises as far as is possible. Cameras are installed throughout the University's sites internally within buildings, externally and in vulnerable public-facing areas. Cameras are not sited to focus on private residential areas.

The CCTV system is operational and is capable of being monitored 24 hours a day, 365/6 days of the year.

The CCTV system is subject to a Data Protection Impact Assessment (DPIA).

Any proposed changes to the CCTV system will be incorporated into the DPIA and it will be re-submitted for review. Any new CCTV Camera installation is subject to a privacy assessment.

Images produced by the recording equipment must be as clear as possible in order that they are effective for the purpose for which they are intended. The standards to be met include:

- Recording features such as the location of the camera and/or date and time reference must be accurate and maintained.
- Cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established.
- Consideration must be given to the physical conditions in which the cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas. Cameras must be properly maintained and serviced to ensure that clear images are recorded and a log of all maintenance activities kept.
- As far as practical, cameras must be protected from vandalism in order to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

2.6 Appropriate Signage

Signs will be placed so that members of staff, students, visitors and members of the public are aware that they are entering a zone which is covered by CCTV cameras. Such signs must:

- Be clearly visible and legible
- Be of a size appropriate to the circumstances
- Contain the following information (where these things are not obvious to those being monitored):
- The name of the Data Controller (i.e. City St George's, University of London)
- The purpose(s) of the scheme
- Basic contact details such as a simple website address, telephone number or email contact

The installation and upkeep of CCTV signage is the responsibility of EE&F.

3. Requests for and Access to CCTV Images and Data

Requests for CCTV footage should be emailed to cctv@city.ac.uk.

In order to locate the images on the University's system, sufficient detail must be provided to allow the relevant images to be located.

In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation, for example for safeguarding, welfare or wellbeing purposes

Requests will be processed in accordance with the Data Protection Legislation and any other relevant legislation or University regulation or policy which may apply.

Where information is requested by the police in pursuit of an investigation unrelated to criminal activity against the premises, personnel of City St Georges University or members of the public, the University will only make such disclosures on receipt of a Police Data Protection Act Form/Personal Data Request Form, and once satisfied of the following:

- That the purposes are indeed those relating to crime;
- That failure to release would prejudice the Police investigation;
- That there is a lawful basis to share such information in data protection law.

In all cases an entry needs to be made in the CCTV Operating Log recording:

- The name and badge number of the Police Officer(s) requesting and receiving the copy of the recording;
- Brief details of the images captured by the CCTV to be used in evidence;
- The crime reference number;
- Date and time the images were handed over to the Police;
- Format in which the information was shared e.g. encrypted USB, secure email.

The EE&F Head of Security is responsible for producing operational guidance and providing training to all Security Officers.

4. UK GDPR Compliance

The University is responsible for and able to demonstrate compliance with the UK GDPR.

CCTV footage being shared with the Police or provided in response to a Subject Access Request (SAR) will be encrypted and transferred securely.

Police requests for data will be processed in the same manner as SARs, under an agreed timeframe.

5. Monitoring Compliance

An annual report on the CCTV system and its use relative to its purpose must be made by the EE&F Department' Head of Security. The system along with all other security functions is subject to City St George's University's Internal Audit process.

All staff involved in the operation of the University's CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.

All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training.

6. Complaints Procedure

Complaints may be made directly to PAF-servicedesk@city.ac.uk, which will follow the department's ISO 9001:2015 Quality Assurance Standard, in conjunction with the Standard Operating Procedure for Complaints Handling.

Complaints can also be made to the Information Assurance Team by email to dataprotection@city.ac.uk. Records of all complaints, and any follow-up action, will be maintained.

Individuals who are not satisfied with how City St George's handles CCTV footage have the right to complain to:

Information Commissioner's Office (ICO). Wycliffe
House
Water Lane
Wilmslow
Cheshire SK9
5AF

By Telephone: 01625 545700
Website: www.ico.org.uk

Annex 1

BS 7958:2015 Surveillance Camera Code of Practice – 12 Guiding Principles

Number	**Principle from the *Surveillance Camera Code of Practice***
1	Use of a surveillance camera system must always be for a specified purpose, which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2	The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3	There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4	There must be clear responsibility and accountability for all surveillance camera system activities, including images and information collected, held and used.
5	Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6	No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7	Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8	Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9	Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10	There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11	When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value
12	Any information used to support a surveillance camera system, which compares against a reference database for matching purposes should be accurate and kept up to date.