CCTV POLICY

Maintained by: PAF Head of Facilities Management

Owned by: Property & Facilities

Last updated: January 2022

Date of next review: January 2023

Current version: v11.5

Contents

POLICY STATEMENT

City, University of London, seeks to ensure as far as is reasonably practicable, the security and safety 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 management of students, staff and visitors.

This Policy document summarises City's approach and should be read in conjunction with applicable privacy notices Its aim is 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, 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. City is a data controller in terms of the Data Protection Act 2018 and the UK GDPR. City is registered with the Information Commissioner's Office (ICO) with the registration number **Z8947127**.

1.1 System Description

The existing system (Genetec) uses IP CCTV cameras. These are currently being upgraded as part of City, University of London's Access Control Project.

"Genetec", is a unified open IP Security platform which allows City to manage CCTV, door controllers and other network infrastructure. 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.

1.2 Purpose of the System

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

City's CCTV system covers the campus 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 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 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'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 our data centre, as this service is hosted on premise. Images are viewable in Security Service areas by all Security staff.

2.1.4 The cameras installed 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 PAF Security Manager is responsible for the operation of City's CCTV system which is supported by IT.

2.2.2 Only the authorised PAF/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 to authorised persons only:

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

2.3.2 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.

2.3.1 For the purpose of viewing CCTV images, an authorised person is defined as an employee or appointed person acting on behalf of City, University of London, with “legitimate interests” for the operational responsibility for either the prevention, investigation, detection of crime, monitoring of security and safety of the premises at City. This is defined by the Data Protection Impact Assessment (DPIA). Those involved in employee disciplinary processes may be authorised on a case by case basis.

2.3.2 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 No images may 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 above, the Head of Facilities Management or the Security Manager (nominated deputy), will be responsible for authorising such a request.

2.4.6 Retained images are to be stored in a secure place to which access is controlled and 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 Head of Facilities Management or the Security Manager (nominated deputy), and any not required for evidential purposes will be deleted.

2.4.8 Requests for CCTV images from third parties such as police, law enforcement and individuals making subject access requests (SARs) should be sent to the Information Assurance Team (IAT) via email to dataprotection@city.ac.uk, with the subject line "Police/Law Enforcement Request" or "SAR". This will generate a request via the IT ServiceNow portal. The request will be allocated to an Information Assurance Advisor and a reference number will be issued.

Security Management will be responsible for other requests, and may consult the IAT for advice, at their discretion.

On receipt of a CCTV footage request, the IAT will:

- View the request as soon as possible and by the end of the next working day after receipt, and
- Start processing Police/law enforcement requests by the end of the next working day after receipt.
- Other third-party CCTV footage requests to IAT will be processed in line with team priorities and statutory compliance deadlines.

There may be times when it is necessary to circumvent this process i.e. an emergency or unavoidable pressures on the IAT. This will be subject to annual review alongside the policy review.

Once the IAT has reached a decision in relation to the request, Security Management will be notified and arrangements made accordingly for the sharing of the data with the requester. This may differ depending on the type of request. The method for sharing the data will be agreed with the 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 for 24 hours a day, every day of the year.

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

Any proposed changes to the CCTV system wll 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, 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 PAF.

3. Requests for and Access to CCTV Images and Data

Information on how to access data for which City is a data controller can be found here:
https://www.city.ac.uk/about/governance/legal/how-to-access-information.

In order to locate the images on the University's system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

Where the University is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

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.

Such disclosures will be made at the discretion of the Head of Facilities Management or Security Manager (nominated Deputy), with reference to relevant legislation and where necessary, following advice from the University's Information Assurance Team.

Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or HR Manager/Advisor, the Head of Facilities Management or Security Manager (nominated Deputy) may provide access to CCTV images for use in staff disciplinary cases.

The Head of Facilities Management or Security Manager (nominated Deputy) may provide access to CCTV images to Investigating Officers when sought as evidence in relation to student discipline cases.

A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

4. Disclosure to the Police

Relevant CCTV footage will be shared with the Police to aid them in the pursuit of investigations into criminal activity against the premises, personnel of City or members of the public. 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
- Thecrime 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

Where information is requested by the police in pursuit of an investigation unrelated to criminal activity against the premises, personnel of City 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 Security Manager is responsible for producing operational guidance and providing training to all Security Officers.

5. 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 accelerated timeframe.

6. Monitoring Compliance

An annual report on the CCTV system and its use relative to its purpose must be made by the PAF Security Manager. The system along with all other security functions is subject to City'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.

7. 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 handles CCTV footage have the right to complain to the Information Commissioner's Office (ICO).

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.