University
for the
Creative Arts

CCTV Policy

Approvedby: University Health, Safety & Wellbeing Committee
Date approved: June 2020
Review period: 3 years
Review Date: June 2023
Owner: Estates & Facilities

CCTV Policy

Contents

1. Policy statement

1.1. This Policy seeks to ensure that the Close Circuit Television (CCTV) system used at the University For The Creative Arts (UCA) is operated in compliance with the law relating to data protection (currently the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018")) and includes the principles governing the processing of personal data as set out in Appendix 1. It also seeks to ensure compliance with privacy law. It takes into account best practice as set out in codes of practice issued by the Information Commissioner and by the Home Office. UCA therefore uses CCTV only where it is necessary in pursuit of a legitimate aim, as set out in clause 1.2, and only if it is proportionate to that aim.

1.2 UCA seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors, contractors, its property and premises. UCA therefore deploys CCTV to:

- promote a safe UCA community and to monitor the safety and security of its premises;
- assist in the prevention, investigation and detection of crime;
- assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings; and
- assist in the investigation of breaches of its codes of conduct and policies by staff, students and contractors and where relevant and appropriate investigating complaints.

1.3 This policy will be reviewed annually by the Security Operations Manager & Director of Estates to assess compliance with clauses 1.1 and 1.2 and to determine whether the use of the CCTV system remains justified.

2. Scope and Objectives of the Policy

2.1 This policy applies to CCTV systems in all parts of UCA's Farnham, Epsom, Canterbury and Rochester campuses and to owned Student residences.

2.2 This policy does not apply to any Webcam systems located in meeting rooms or lecture theatres operated by Schools or IT, which are used for the purposes of monitoring room usage and to assist with the use of the audio visual equipment.

2.3 No system shall be installed or operate without the prior approval of the Director of Estates and the submission of a Privacy Impact Assessment to the University Secretary.

2.4 This policy applies to all UCA staff, contractors and agents who operate, or supervise the operation of, the CCTV system including Security Management and Staff, Facilities Management and Staff and Accommodation Management.

2.5 This policy has been prepared for the guidance of the managers and operators of the CCTV system. Its purpose is to ensure that the CCTV system is used to create a safer environment for staff, students and visitors to the University, consistent with the obligations on the University imposed by the GDPR and Data Protection Act 2018.

3. Roles and Responsibilities

3.1 The Chief Operating Officer has the overall responsibility for this policy, but has delegated day-to-day responsibility for overseeing its implementation to the staff identified in this policy. All relevant members of staff have been made aware of the policy and have received appropriate training.

3.2 The Security Operations Manager is responsible for ensuring that the CCTV system including camera specifications for new installations complies with the law and best practice referred to in clause 1.1 of this policy. Where new surveillance systems are proposed, the Security Operations Manager will consult with the University Secretary to determine whether a prior privacy impact assessment is required.

3.3 Only the appointed maintenance contractors for UCA's CCTV systems are authorised to install and/or maintain it.

3.4 The Security Operations Manager is responsible for the evaluation of locations where live and historical CCTV images are available for viewing via the network software. The list of such locations and the list of persons authorised to view CCTV images is maintained by the Security Operations Manager.

3.5 Changes in the use of UCA's CCTV system can be implemented only in consultation with the University Secretary and the University Solicitor.

4. System Description

4.1 UCA has installed CCTV surveillance systems which are owned by the University and the control centres/monitoring stations are currently staffed by directly employed and contracted security staff.

4.2 The CCTV systems have been installed to prevent and detect crime and to provide a safe public environment for the benefit of those who live or work within the University or visit it, consistent with respect for individuals' privacy. These objectives will be achieved by the use of the system, to:

- assist in the prevention or detection of crime;
- provide evidence of crime;
- deter those having criminal intent; and
- promote public safety and give confidence to staff and visitors that they are in a secure environment.

Even where a potential or actual crime is not involved, the system will help to deter, detect and take action, as appropriate, in relation to other non-criminal behaviour which is either unlawful, anti-social and/or in breach of University rules and/or policies.

Cameras will be deployed in areas that offer maximum effectiveness in relation to their purpose as defined by this policy whilst maintaining regard for the right to privacy.

Cameras should not be hidden from view and prominent signage is to be located at all the site accesses and entrances to inform the public and members of the University, both of the presence of the system and its ownership and purpose.

To ensure privacy, the cameras are prevented from focusing or dwelling on adjacent public or private property or the windows of student residential accommodation and this will be demonstrated on request. We aim to operate the scheme with a high regard for the privacy of the individual.

The CCTV system has the capability of recording sound, but the University chooses not to use this option. If they elect to then a further Privacy impact Assessment will be completed, and notices would make this clear in the determined areas.

Images captured on camera will be transmitted to the appropriate DVR (Digital Video Recorder) where they will be recorded on the DVR internal hard drive for use in accordance with this Policy.

4.3 Farnham

Porters' Lodge

The Porters' Lodge is the main monitoring station for all CCTV apart from the two stand-alone systems in the Stores and the Student Union. It is staffed by external security guards from 1800 to 0600 Monday to Friday and 24 hours at weekends, Bank Holidays and University close down periods. During the normal working day Facilities Assistants staff the Porters' Lodge at short intervals throughout the day, mainly for giving out parcels and processing post and the monitors are not monitored. The CCTV in this area is open for view to all who enter the Porters' Lodge. The Porters' Lodge is locked at times when unmanned. The control centre equipment is for purposes of monitoring and there is no facility to manipulate, stop or save images for downloading.

There are two stand-alone CCTV systems. One is within the Equipment Stores (G08) which has no monitor and images are viewed only from the Resource Manager's, Security Operations Manager, Facilities Manager and Director of Estates PCs. The other system is within the Student Union/Refectory. This is housed in the Box Office and is only accessible by the Security Operations Manager, Facilities Manager and Director of Estates.

Reception

A monitor is housed on the Reception desk and the DVR is locked away in the walk-in cupboard by the side of Reception. The Reception is manned from 0830 to 1730 Monday to Friday and when open on Saturdays by temporary staff who do not have access to the cupboard. The area is locked down and alarmed when closed.

Gateway

A monitor and the DVR are located in a cupboard behind the Reception desk which has a pull over cupboard door so the equipment cannot be viewed. The Gateway Services are manned from 0800 to 2000 Monday to Friday and 1000 to 1700 Saturdays and 1300 to 1700 Sundays. The area is locked down and alarmed when closed.

John Luard

The monitor and DVR are located in the Technicians' Office in the walk-in cupboard. The monitor can be seen by those entering the office. The area is not monitored for specific times and if the technicians are not in the room then the room is locked.

Accommodation Office (Student Village CCTV)

A monitor and the DVR are housed in a walk-in cupboard within the Technicians' Office. This office is staffed throughout the day Monday to Friday. The room is locked down when not in use. The building is locked down and alarmed when closed.

Equipment Store (G08)

This is a stand-alone CCTV system with the DVR being locked away in G08 with access only by the Resource Managers, with no monitor. The room is locked down throughout the day with controlled access. The building is locked down and alarmed when closed.

Student Union/Refectory

This is a stand-alone system with the DVR and a monitor housed within the Box Office which is locked throughout the day with access only by the Security Operations Manager, Facilities Manager and Director of Estates. The system is only monitored at times when the Student Union is open and for their events. The building is locked own and alarmed when closed.

Craft Study Centre

A monitor is housed on the Reception desk and the DVR is locked away in the IT Machine Room which has controlled access. The Reception is manned from 1000 to 1700 Tuesday to Friday and 1000 to 1600 on Saturdays. The building is locked down and alarmed when closed.

Images recorded on these systems can be accessed by The Facilities Manager, Assistant Facilities manager, Security Operations manager and Director of Estates.

4.4 Epsom

The system at Epsom includes the Main Campus, LLRC, PC5, Wilberforce Court and 2 Ashley Road. Images captured on camera are monitored either by stand-alone monitoring stations or the main control centre (Security Office). The Main Campus system comprises a digital IT network-based system with monitoring and recording facilities.

The Security Room is staffed by security from 1715 to 0700 Monday to Friday and 24 hours at weekends, bank holidays and University closures. Facilities Assistants enter the locked security office during the day to check the DVRs are operational and obtain security keys. The DVR units are locked in a steel security cabinet.

Images recorded can be accessed by The Facilities Manager, Assistant Facilities manager, Security Operations manager and Director of Estates

4.5 Canterbury

The CCTV Control Centre in the Caretakers' Office (Room D0.11) is monitored at short intervals throughout the day Monday to Friday during the core hours of 0900 to 1715. The contract Security Guard monitors the Control Centre 1715 to 0700 on weekdays and 24 hours at weekends, Bank Holidays and University closures.

The system at Canterbury covers the Main Campus, LLRC and the student halls at Ian Dury House. Images captured on camera are monitored in the Main Control Centre located in the Facilities Assistant's Office. The Control System comprises monitoring and recording facilities and is not manned. However, the Caretakers have access to the station during the core opening hours of 0900 to 1715. During out of hours, weekends and Bank Holidays, the contract Security Guard monitors the CCTV. The video recorder is capable of providing 31 days of continuous recording, after which they are overwritten. Images recorded can be accessed by The Facilities Manager, Assistant Facilities manager, Security Operations manager and Director of Estates.

4.6 Rochester

The CCTV control centre in the Facilities Assistants' office is not staffed but the Facilities Assistants have access to view live images. As the campus is shut down at 2100 hours on weekdays, weekends and Bank Holidays, the control centre is not manned and there are no remote monitoring facilities.

The system at Rochester includes the South and North blocks. The system comprises a digital IP system connected to a PC and screen for monitoring and recording of images. There is a stand-alone system in Reception which is for monitoring only, with no recording of images.

Images captured on cameras are monitored in the main control station in the Facilities Assistant's Office. The viewing software is also installed on a PC in the Facilities Manager's Office. The main control station for the IP system is password protected and secured. Only the Assistant Facilities Manager and Facilities Manager (C&R) have access to this station.

The digital video recorder is capable of providing 31 days of continuous recording, after which they are overwritten. The system consists of full dome cameras triggered by movement sensors, static and roving cameras.

Images recorded can be accessed by The Facilities Manager, Assistant Facilities manager, Security Operations manager and Director of Estates.

5. Control Centre / Monitoring Station Administration and Procedures

5.1 A CCTV logbook will be maintained and kept securely by the Facilities Manager. Brief details of incidents will be noted together with any consequential action taken, i.e. who was notified of the incident and when. This will be a separate measure to the University's incident reporting procedure.

An incident is defined for the purposes of this policy as any event or occurrence for which the recording and viewing of Digital Video Recordings is a justified and proportionate enquiry as determined by the scope and objectives set for the deployment of CCTV (See 1.1 and 1.2).

It is recognised that the images obtained are sensitive and subject to the law on Data Protection. All copies will be handled in accordance with the University's working procedures, which are designed to ensure the integrity of the system. The Security Operations Manager and Facilities Manager on each campus will be responsible for the development of and compliance with the working procedures in the control centres/monitoring stations/recording facilities.

Images and footage will only be reviewed at the request of the Police or with the authority of the Director of Estates, The Security Operations Manager or the Facilities Manager, or, where it is not reasonably practicable to contact them, a member of the Leadership Team. Copies of recorded footage or images will only be made for the purposes of crime detection, to assist with the investigation of University complaints relating to breaches of conduct or policy or where required or permitted by law.

5.2 Communications

When CCTV is monitored, emergency procedures may be used in appropriate cases to call Police, Fire Brigade or Ambulance services.

5.3 Staff

All staff will be made aware of the sensitivity of handling CCTV images and recordings. Suitable vetting of control centre/monitoring station staff and managers will be carried out.

The Security Operations Manager and the Facilities Manager will ensure that all staff, including relief staff using systems, are fully briefed and trained in respect of all functions, both operational and administrative arising within the CCTV system. Training by camera installers may also be provided.

Training on legal data protection requirements must be given to staff required to work in the control centres/monitoring stations. In the event that staff operating the system are sourced from external providers, the University will ensure they are Security Industry Authority (SIA) licensed where required.

5.4 Recording

The control centre/monitoring station systems/recording facilities are supported by Digital Video Recording facilities, which will function throughout operations. Images are recorded in 'real time'.

Image recordings are captured on each DVR through an internal hard drive within the DVR and images are date and time stamped. Recorded images will be retained for 31 days from the date of recording.

In the event that the system has captured recordings of an incident and is required for evidence, it will be downloaded and burnt to CD or USB device and clearly marked and if not signed over to the Police will be kept securely by the Facilities Manager, retained for a period recommended by the Police or by the University Secretary. The University will carry out regular checks to monitor compliance with the retention requirements.

CCTV downloads will be held for a period of time no longer than necessary for any follow-up investigations before being destroyed and a record made of their destruction in the CCTV logbook.

6. Digital Video Recording (DVR) Procedures

6.1 Control and Management of Digital Video Recorders

All DVRs belong to and remain the property of the University. Handling procedures are to ensure the integrity of the image information held.

Each DVR will be dedicated to a specific location and will be held securely. Each separate DVR records images 24 hours a day and this is held on the DVR on an internal hard drive for 31 days.

The operational DVR is maintained every six months and any repairs/downtime will be reported to the respective CCTV installer company as soon as a fault/repair is identified.

6.2 Access to Recordings and Images

Generally, a request for access to a recording or images will only be granted if it comes from the Police. Police requests will arise in a number of ways, including:

- regular requests for a review of recordings, in order to trace incidents that have been reported;
- immediate action relating to live incidents e.g. immediate pursuit;
- for major incidents that occur; and
- a request from an individual Police Officer seeking to review a recording within the control centre/monitoring station.

Requests for access to recordings or images from persons other than the Police will be considered on a case-by-case basis. Such requests, which must be recorded on the standard University's access request form, will be considered by the Director of Estates and Facilities, the Security Operations Manager or the Facilities Manager. Access to recordings or images in these circumstances will only be granted where it is compliant with the rights of the individual and obligations placed on the University by the GDPR and the Data Protection Act 2018.

All requests must normally be made within 30 days of the incident in question and will be responded to within 40 days of receiving the required request form.

Release of recordings or images will be permitted for a period which will be long enough only for authorised third parties to view them or - where they may be required for evidence - no longer than a Court may require them. Recordings or images that may be required by the Police are to be inhibited from being manipulated and only the specific recordings of the incident burnt to CD or downloaded to digital storage device. Recordings will not be released except in these circumstances.

All recordings and images are time and date stamped to ensure the footage can be used in evidence; the following procedures will be followed:

- When requested by Police the recording requested should be burnt to two CDs or USB devices and these are to be sealed in separate tamper proof envelopes which are clearly marked "MASTER" and "WORKING COPY" and date stamped. These CDs or devices and envelopes are to be provided by the Police. This should be entered into the CCTV logbook with an appropriate reference number;
- On collection, the requesting Officer should present a Data Protection Act form which is signed and have the Police officer's name and Force Identification Number available;
- This form, along with the Police officer's details, are to be entered into the CCTV logbook;
- The Police officer must then sign for the envelope next to the entry in the CCTV logbook before taking the envelope away;
- A photocopy of the incident report, if relevant, will be issued along with the DVR. The original of the incident report will be retained securely.

6.3 Viewing of Recordings

Software for the CCTV systems is held on the Facilities Manager's computer, the Assistant Facilities Manager's computer, the Security Operations Manager's computer, and the Director of Estates' computer and is restricted. These persons under normal circumstances are the only persons who have access to the software and are able to view images.

If a request is made by the Police or any other person to view recordings, a record will be made of the request in the CCTV logbook.

If a recording is to be made available to the Police or other authority, the event will be noted in the CCTV logbook and the details and signature of the recipient obtained. His or her name and identification will be printed in the CCTV logbook along with the date and time removed and the date and time returned (if applicable).

6.4 Image Prints

Any prints taken from recordings are subject to the same controls and the same principles of Data Protection as other data collected. They may only be obtained to assist the identification, apprehension and prosecution of alleged offenders, during staff training and for other purposes consistent with the purposes of the CCTV system set out in this policy.

Image prints will normally be supplied to the Police upon reasonable written request where permitted by the GDPR and DPA. Any requests for viewing image prints other than a police request will be considered by the Facilities Manager in liaison with the Assistant Directgor of Estates and Facilities in consideration to relevant legislation under the GDPR and DPA 2018 and Information Commissioners Guidance (ICO) guidance and recommendations.

All image prints produced must be recorded along with the identity of the requesting person, date and other appropriate information in the CCTV logbook.

7. Digital Image prints

7.1 Control of Images

All images recorded are automatically erased after 31 days, subject to any ongoing requirements for the images in accordance with paragraph 6.2 of this policy.

7.2 Access to Images

The system only permits viewing from the designated terminal and by authorised personnel with the required password.

Requests for viewing images from the Police or other authorised person will be handled in the same manner as for recordings under paragraphs 6.2 and 6.3.

8. System Maintenance

8.1 The system maintenance is contracted with the respective system installers. The whole of the CCTV system and cameras are maintained on a six-monthly basis. Response for callouts is within four to eight hours, dependent on the time of day, or will be the next working day. Maximum anticipated downtime is 24 hours, dependent on the severity of fault/breakdown. DVR and cameras are refurbished or replaced upon major breakdown. Any fault call-out will be reported in the CCTV logbook.

9. Complaints

9.1 Estates and Facilities are responsible for the operation of the CCTV system, and for ensuring compliance with this Policy. Breaches of the policy by control centre/monitoring station staff will constitute matters of discipline under the relevant conditions of employment. Staff members of the University, or members of the public, who have concerns or complaints about the operation of the system or compliance with this policy should address them, in the first instance, to the Security Operations Manager or Campus Facilities Manager. Alternatively, concerns may be raised with the Director of Estates and Facilities. All formal complaints received with respect to the CCTV system will be recorded, enquiries instigated and wherever possible a response provided within 30 days. These rights do not alter the existing rights of the University's staff under the relevant grievance or disciplinary procedures.

Any student complaints or concerns about the CCTV system or compliance with this policy should be dealt with in accordance with the Student Complaints Policy.

A report will be issued annually evaluating the effectiveness of the CCTV system in comparison with its stated objectives, reviewing the documented procedures, any recorded complaints and outcomes, any relevant changes in applicable law, guidance and best practice and incorporating recommendations, if necessary, for improvements. Copies of the report will be issued to all data protection officers and will be available to all other members of the University and to the public.

10. Useful links

The Information Commissioner's Office Code of Practice for CCTV can be found here: https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

Appendix 1

Principles relating to the processing of personal data under the Data Protection Act 2018 and General Data Protection Regulation (GDPR)

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; and

f) 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.