University of Cambridge

CCTV Code of Practice

2018/19

Prepared on behalf of the Head of Estates Facilities

Contents – Index

Code of Practice

1. Introduction

1.1 The University of Cambridge (the "University") is the owner of a number of closed circuit television systems (CCTV) currently installed in and on University sites and buildings; in addition the systems may at times incorporate ANPR, body worn and covert cameras as defined below.

1.2 This Code of Practice applies only to University owned systems which together will collectively be known as the CCTV systems.

1.3 Cameras are located in various areas around the University Estate including roadways, car parks, buildings, vulnerable public facing offices and walkways, academic buildings and retail and licensed premises.

1.4 There are several types of camera –
Overt Fixed – these record uncontrolled images (e.g. reception desk, doors etc.)
Overt pan, tilt, zoom (PTZ) – these are controllable cameras that can follow vehicles or subjects when required.
Covert cameras – temporarily fitted cameras which can be used in areas not previously covered by CCTV but the scene of serious or persistent criminality.
ANPR – these record vehicle number plates together with a date and time stamp.
Body worn – these may be used by security staff when on late night patrols and dealing incidents such as drunkenness, violence and anti-social behaviour.

1.5 The cameras provide images that are suitable for the specified purposes for which they are installed (i.e. monitoring, detection, prevention, recognition and identification) and will be regularly checked to ensure images remain fit for purpose.

1.6 Images are recorded both:

i. Locally within departments - these are viewable by a limited number of management and staff who have the facility to monitor cameras sited within their own area of responsibility.
ii. Centrally - on servers in the University Security Control Centre (USCC) - these are viewable centrally by University Security staff and for the purposes of this Code will be referred to as the central CCTV system.

2. Objectives for the Use of all University CCTV Systems

2.1 The objectives for the use of the various CCTV systems are to:-

i. Assist in providing a safe and secure environment for the benefit of those who might work, study, live in or visit the University.
ii. Reduce crime and the fear of crime by reassuring students, staff and visitors.
iii. Deter and detect crime, public disorder and anti-social behaviour.
iv. Identify, apprehend and prosecute offenders in relation to crime, public disorder and anti-social behaviour.
v. Monitor crowd movements during University events.
vi. Monitor and assist with traffic management.
vii. Assist in the monitoring and deployment of security staff during normal duties and emergency situations.
viii. Protect security staff from undue threats and violence whilst going about their duties.
ix. Obtain evidence for use in the investigation of criminal activity, breaches of health and safety legislation and, where appropriate, breaches of student and staff disciplinary procedures.
x. Provide Public Agencies (such as the Police, Health and Safety Executive etc.) and the University with evidence upon which to take criminal, civil and where permissible disciplinary action respectively.

3. Procedural and Administrative Notes

3.1 The Senior Security Operations Manager retains overall responsibility for the central CCTV system and delegates the day to day management to the Deputy Security Operations Manager. It is the Security Operations Managers' responsibility to ensure that all CCTV within the University is managed in line with this Code of Practice, the current CCTV Code of Practice produced by the Information Commissioner's Office, the current Surveillance Camera Code of Practice issued by the Home Office and General Data Protection Regulation .

3.2 Heads of Department are responsible for any local CCTV systems in their own domain and the implementation and application of these codes of practice. They should ensure any systems for which they are responsible are managed in line with this code as well as the current CCTV Code of Practice produced by the Information Commissioner's Office, the current Surveillance Camera Code of Practice issued by the Home Office and Data Protection legislation.

3.3 All images produced by the systems remain the property and copyright of the University

3.4 The purpose of CCTV is not to monitor staff activity, although it may be used to establish the facts of any crime, public disorder or anti-social behaviour including those potentially perpetrated by employees. The University will only use images in a staff disciplinary case when there is an allegation of gross and other serious misconduct and where there is a likelihood that the images will either prove or disprove the allegation. In all such cases the Investigating

Officer or HR Schools Team will formally request access to images from the relevant controller of the CCTV system only after permission has been given by the Director or Assistant Director of HR. It is the responsibility of the Security Operations Manager to ensure all such requests are in accordance with 3.1 above. As with all personal information, where access is given, the confidentiality of these images and who is able to access them will be closely controlled by all involved in accordance with General Data Protection Regulation.

3.5 Likewise the images will only be sought as evidence if a serious student discipline case is being conducted through the formal procedures set out in the University's Statutes and Ordinances.

3.6 Covert cameras will be used on rare occasions when a serious or persistent criminality is taking/has taken place (e.g. thefts in the same area not fitted with CCTV) and all other physical methods of prevention exhausted. Authority of the Senior Security Operations Manager must always be sought before installing any covert cameras

3.7 Body worn cameras will be used by University Security staff during patrol duties and recordings downloaded when evidence is required. The down loads will only be conducted by authorised security staff and the cameras will be cleansed following each shift used. Officers wearing these cameras will disclose verbally, when approaching persons, that they are being video and audio recorded.

3.8 Small Unmanned Aircraft (Drones) are the subject of CAA Regulations. The use of such aircraft to obtain photographic images and data on or over the University estate will not only be subject to CAA Regulations, but must also comply with the General Data Protection Regulation and CCTV Codes of Practice cited in this document. Further reference can be obtained through the University's Drone Policy.

3.9 The objectives outlined in Section 2 of this code will be closely followed when assessing the requirements for new CCTV installations. Similarly, if designated usage of any area changes it will be necessary to assess whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation.

4. University Security Control Centre

4.1 The University Security Control Centre (USCC) is capable of receiving images from throughout the estate. It is staffed 24 hours a day by uniformed University Security Patrollers. In addition some departmental managers and staff are able to view local images by way of direct and remote viewer cameras linked to the network.

4.2 The USCC is also equipped with a Home Office licensed radio system linking the Centre with uniformed Security Patrollers and departmental staff who provide security patrols and are able to respond to incidents identified on the CCTV monitors.

5. Data Protection

5.1 This Code of Practice reflects the spirit and guidance issued by the Information Commissioner's Office as documented in the current CCTV Code of Practice and the Surveillance Camera Code of Practice issued by the Home Office and will not be used to invade the privacy of any individual, residence, business or other private premises, buildings or land.

5.2 The University is committed to complying with the requirements of General Data Protection legislation and will operate all CCTV systems in accordance with the data protection principles and the guiding principles set out in the CCTV Surveillance Camera Commissioners' Office 'Code of Practice'.

5.3 All members of Security staff involved in operating University CCTV systems will be SIA CCTV Operator trained and will be made aware of the objectives of this Code as set out in Section 2 and will be permitted only to use the system to achieve those objectives.

5.4 All members of staff involved in operating CCTV systems will be provided with access to this Code for reference and compliance purposes.

5.5 The University recognises the importance of strict guidelines in relation to access to and disclosure of recorded images and all members of Security staff who are SIA trained are permitted access or to download CCTV recordings. These restrictions relating to this are set out in this Code and the rights of individuals under Data Protection legislation.

5.6 Only SIA trained Security staff are permitted to transport CCTV recording between buildings.

6. Administration

6.1 In respect of the central CCTV system, it will be the responsibility of the Senior Security Operations Manager or in their absence their deputy to:–

i. Select camera sites and initial areas to be viewed and ensure that a suitable assessment of the privacy implications is completed in advance of selecting new sites/areas.
ii. Be responsible for compliance with General Data Protection Regulation insofar as it impacts upon the use of CCTV systems.
iii. Take responsibility for control of the images and make decisions on how these can be used.
iv. Ensure the system is secure and only viewed by authorised persons.*
v. Ensure that the procedures of this Code of Practice comply with the current CCTV Code of Practice produced by the Information Commissioner's Office and the current Surveillance Camera Code of Practice issued by the Home Office.

vi. Maintain the central CCTV system incident log and records of Police or other statutory requests for images.
vii. Make bi-annual checks to establish that nominated managers still require viewing rights of the system in line with the above objectives.
viii. Ensure adequate signage is erected.
ix. Regularly evaluate the system to ensure compliance with the latest legislation and national Codes of Practice

* Authorised persons include:-

- Security staff
- Other University staff tasked with monitoring, security, safety, anti-social behaviour and relevant areas of legal compliance.
- Police Officers
- Other Statutory Officers e.g. Health and Safety Executive Officers
- Management/Investigating Officers, Proctors and HR staff with a legitimate reason for accessing images.
  When appropriate in formal investigations, members of staff, trade union officials and colleagues accompanying them, as well as students facing disciplinary action and their accompanying representatives.

6.2 In respect of all University systems it will be the responsibility of the Senior Security Operations Manager to:-

I. Clearly communicate the specific purposes of the recording of and use of images and objectives to all relevant staff.
II. Ensure that the practices and procedures comply with the current CCTV Code of Practice produced by the Information Commissioner's Office and the current Surveillance Camera Code of Practice issued by the Home Office.
III. Carry out annual audits to check that Faculties and Departments comply with the practices and procedures set out in the Codes of Practice mentioned in Paragraph ii. above.
IV. Ensure that all disclosure requests received from the Police or other investigatory bodies (e.g. Health and Safety Executive) are held for future reference for a suitable period.
V. Ensure that all data and images are erased after a period of 3 months unless retained for evidential purposes.
VI. Ensure that camera sites and areas to be viewed follow the 12 principles of the Surveillance Camera Code of Practice issued by the Home Office.

6.3 It will be the responsibility of the individual operating officer, including authorised departmental staff, to –

i. Select appropriate images to be recorded on controllable cameras (PTZ) so as to comply with the objectives outlined above.
ii. Ensure that targeting of individuals with the cameras is only conducted when there is reasonable suspicion that the person falls within one of the objectives set above e.g. committing a criminal offence.

iii. Not to view into private property and be mindful of privacy within any accommodation.
iv. Complete a CCTV incident log as appropriate.

7. Storing and Viewing of Images

7.1 All images recorded digitally on University cameras, both centrally at the University Security Control Centre or remotely within their respective Departments, are stored on computer/server hard drives and although the images can be searched it is not possible to tamper with or alter them. There are also some smaller non-digital departmental CCTV systems which record images onto digital storage or other portable media; these are also protected against tampering and alteration.

7.2 In the event of the Police requiring images they can be 'exported' onto a DVD (or other appropriate portable media) for evidence in court, on receipt of the appropriate disclosure documentation.

7.3 CCTV images should not be kept for longer than is strictly necessary to meet the purpose of the recording. The central CCTV system images over-record after a maximum 28 days, dependant on the image quality being recorded, however any relevant images can be 'locked' on the hard drive for future reference.

7.4 All images and data on both the central and departmental systems will be erased after a maximum of 3 months unless required for evidential purposes.

7.5 Locked images must be reviewed on a 3 monthly basis and any not still required for evidential purposes should be deleted. Images that have been retained for evidential purposes should be deleted as soon as they are no longer required

7.6 In the USCC the viewing of live images on monitors is restricted to Security Managers, Supervisors and Security Patrollers/Control Room Operators. Other authorised persons may also view these images once they have signed the visitor's book.

7.7 In Departments images must be viewed confidentially in secure private offices.

7.8 Body worn video evidence relating to crimes with police involvement should be kept for a period of 3 months before deletion. All other footage should be kept for 31 days before deletion unless there is a valid reason for extended retention.

7.9 All images (including especially portable media) shall be sufficiently protected to ensure that they do not fall into the wrong hands. This will include technical, organisational and physical security. A record will be kept to show to whom any copy is supplied.

7.10 Requests to view images or for image disclosure should be made in writing to the Senior Security Operations Manager or the relevant Head of Department.

8. Disclosure

8.1 The following guidelines will be adhered to in relation to disclosure of images:-

i. Will be in line with the above objectives.
ii. Will be controlled under the supervision of the Senior Security Operations Manager or his/her deputy or relevant Head of Department and where necessary in consultation with the University Data Protection Office.
iii. A log will be maintained itemising the date, time(s), camera, person copying, person receiving and reason for the disclosure.
iv. The appropriate disclosure documentation from the Police or other outside agencies will be filed for future reference.
v. Images must not be forwarded to the media for entertainment purposes or be placed on the internet.
vi. Images must not be copied in any way, e.g. photographed, downloaded or printed for use other than described in the objectives.
vii. Images will only be released to the media for identification purposes in liaison with the Police or other law enforcement agency.
viii. The method of disclosing images should be secure to ensure they are only seen by the intended recipient.
ix. Images of third parties not relevant to the investigation should be obscured where possible to prevent unnecessary identification.

Even if a system was not established to prevent and detect crime, it would still be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime.

8.2 Any other requests for images should be routed via the Senior Security Operations Manager or his/her Deputy, as disclosure of these may be unfair to the individuals concerned. In some limited circumstances it may be appropriate to release images to a third party, where their needs outweigh those of the individuals whose images are recorded.

8.3 The University has discretion to refuse any third party request for information unless there is an overriding legal obligation such as a court order or information access rights. Once an image has been disclosed to another body, such as the police, then they become the data controller for their copy of that image. It is their responsibility to comply with General Data Protection Regulation in relation to any further disclosures.

9. Signage

9.1 Signage has been erected at the main entrances to the University estate and at other locations where CCTV (including ANPR) is in use informing that them that CCTV surveillance is in operation.

9.2 The signs contain details of the University and a contact number for Security.

9.3 It is the responsibility of the Senior Security Operations Manager to advise departments to ensure adequate signage is erected. Departments are required to implement the Security Operations Managers instructions where it is considered there is insufficient or inappropriate signage displayed to satisfy regulatory or legal requirements.

10. Subject Access Rights

10.1 Individuals whose images are recorded have a right to request access to copies of images of themselves and, unless they agree otherwise or an exemption applies, to be provided with a copy of the images. All such requests will be handled and logged centrally by the Senior Security Operations Manager in consultation with the University Data Protection Office and should be passed to data.protection@admin.cam.ac.uk upon receipt. Staff should not attempt to handle or answer these requests themselves.

10.2 The Senior Security Operations Manager and the University Data Protection Office will process such requests in accordance with the relevant legislation and best practice. In particular, if images of third parties are also shown with the images of the person who has made the access request, consideration will be given as to whether there is need to obscure the images of the third parties.

11. Freedom of Information

11.1 The University may receive requests under the Freedom of Information Act 2000 (FOIA) for CCTV images. All such requests are dealt with centrally by the University FOI Office and should be passed to them upon receipt at foi@admin.cam.ac.uk

11.2 The University FOI Office will process such requests in accordance with the relevant legislation and best practice. In particular, consideration will be given to the privacy rights of any identifiable individuals.

12. Use of CCTV Systems

12.1 All security staff and other authorised users (as defined in paragraph 6 above) must read this Codes of Practice prior to being instructed on the operation of any system.

12.2 Each system can be used to observe the University estate and areas under surveillance and identify incidents that require a response; the response should be proportionate to the incident being witnessed. On some occasions the deployment of a Security Officer may be sufficient

on other occasions contacting the Police to respond may be the appropriate action.

12.3. Such surveillance should be in accordance with the stipulated objectives.

12.4 Whenever a response is required a log should be commenced on the USCC incident reporting system.

12.5 Viewing monitors should be password protected and switched off when not in use to prevent unauthorised use or viewing.

13. Complaints

13.1 Complaints received in relation to the use of CCTV systems should be made to the Senior Security Operations Manager who will consult with appropriate Senior Officers and where relevant, investigate the allegation or complaint under the University's procedures.

13.2 Complaints in relation to the disclosure or supply of images should **be** made in writing to the Senior Security Operations Manager.

14. Changes to this Code of Practice

14.1 Changes to this Code are to be ratified by the Registrary.

Appendix A – Glossary of Terms

Terms	Meaning
ANPR	Automated Number Plate Recognition
CAA	Civil Aviation Authority
CCTV	Closed Circuit Television System
DVD	Digital Video Device
FOIA	Freedom of Information Act
HR	Human Resources
PTZ	Pan Tilt Zoom
SIA	Security Industry Authority
USCC	University Security Control Centre