Security Services

Codes of Practice

Closed Circuit Television (CCTV)

Review date: Oct/Nov 2019

Contents

Appendix 6 – Disclosure - request form
Appendix 7 - Operational Requirement form for new cameras
Appendix 8 - Operational Requirement form for OUSS deployable camera

1. Introduction

The University of Oxford Security Services operates a Closed Circuit Television (CCTV) system. The primary monitoring facility is located at the Old Observatory and secondary monitoring facilities are located at the satellite control room at Old Road Campus (ORC). The CCTV system is the subject of a regular maintenance programme.

For the purposes of this document operator of the CCTV system is Oxford University Security Services (OUSS) and the Operational Manager (OM) is OUSS Operations Manager. Under the Data Protection Act (DPA), the 'data controller' for the images produced by the system is the University of Oxford. The University of Oxford CCTV systems are registered with the Information Commissioners Office (ICO) and the registration number is: Z575783X

2. CCTV System objectives

The objective of the OUSS CCTV system is the prevention and detection of crime and the safety of staff, students and visitors

3. General Data Protection Regulations 2018, Freedoms of Information Act 2012 & Human Rights Act 1998 (*Article 8 Respect for Private and Family Life)*

(i) Data Protection Principles

As the data controller for the System, the University is obliged to comply with the data protection principles embodied in the General Data Protection Regulations. The 6 key principles are:

1. Lawful, fair and transparent *(personnel data needs to be processed lawfully, fairly and in a transparent manner)*

   OUSS meets this requirement achieving voluntary certification with the Surveillance Camera Commissioners Codes of Practice and has published the following documents:

   - *CCTV Codes of Practice*
   - *Privacy Notice*
   - *Data Protection Impact Assessment (formerly PIA)*
   - *CCTV warning signs are clearly displayed to indicate the presence of CCTV*
   - *Annual systems audit to ensure there is a legitimate reason and pressing needs for a cameras continued deployment.*

2. Purpose limitation *(Personal data should only be used in the way set out in privacy notices)*

   OUSS meets this requirement by publishing a Privacy Notice, defining objectives for the System in this policy and carryout annual audits to review the continued justification for deploying individual cameras in relation to the objectives.

3. Data minimisation *(We should not collect, store or use more data than is strictly necessary)*

   OUSS meets this requirement by ensuring that the routine retention of recorded material does not exceed 30 days.
4. Accuracy *(Personal data needs to be correct and up-to-date)*

   OUSS meets this requirement by ensuring through regular maintenance that the System is capable of producing images of sufficient quality to be admitted as evidence in legal proceedings.

5. Storage limitation *(We should only keep people's information for as long as necessary)*

   OUSS meets this requirement by ensuring that the routine retention of recorded material does not exceed 30 days.

6. Security *(We need to keep people's personal data safe and secure and to make sure that it is not lost, destroyed or damaged)*

   OUSS meet this requirement by formulating and implementing appropriate technical and organisational policies and procedures.

(ii) Protection of Freedoms Act 2012 & Surveillance Camera Commissioner's Codes of Practice 2013

The University of Oxford is not defined within the Code of Practice as a 'relevant authority' and as such are not obliged to implement the Codes. However, Security Services has achieved voluntary certification with the Surveillance Commissioners Codes of Practice.

The Code sets out 12 guiding principles that apply to all local authority surveillance camera systems in public places are designed to provide a framework for operators and users of surveillance camera systems to define the legitimate reason and pressing need for CCTV cameras promoting proportionality and transparency in their use..

The 12 guiding principles of the Surveillance Camera Code of Practice are:

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 image 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. (Refers to ANPR and facial recognition – not applicable)

(iii) Human Rights Act 1998

The University recognises that relevant authorities and those organisations carrying out the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998, and consider that the use of CCTV across the University precincts is a necessary, addressing a legitimate aim and pressing need; being a proportionate and suitable tool to help prevent and detect crime, reduce fear of crime and improve public safety. This is supported by the use of 'operational requirement' documents which relate to all cameras on the system outlining the justification for their deployment.

The University of Oxford OUSS CCTV System will be operated with respect for all individuals. It is recognised that the operation of the CCTV System may be considered to infringe on the privacy of individuals. The University recognises that it has a responsibility to ensure that the scheme will only be used as a proportionate response to identified problems and be used only in so far as it is necessary to support the systems objectives.

4. CCTV Operators

All CCTV operators and authorised staff, including managers, have received training relevant to their role in relation to the General Data Protection Regulations, Human Rights Act and the Protection of Freedoms Act – Surveillance Camera Commissioner's Codes of Practice. Operators training will be subject to the annual audit and refresher training will be delivered by the internal trainer. OUSS CCTV operators are not required to be SIA licensed because they are employed directly by the University.

OUSS CCTV operators have a unique user name and password that has to be entered correctly into the CCTV operating system before they can operate the cameras.

5. Discipline

CCTV operating processes and procedures are available for staff to consult. All staff sign a CCTV code of ethics and confidentiality document following their CCTV operators training and agree they understand the processes, procedures and their legal responsibilities when operating the cameras. (Appendix 1)

Disciplinary action will be taken if a CCTV operator breaches local or legal operating requirements.

6. CCTV Suite & Security Control Room(s)

The main CCTV suite and satellite security room are located in secure areas in university buildings where authorised access is controlled through programmable access control systems. Unauthorised personnel can only enter the security room(s) by prior arrangement, they must be accompanied and sign in and out of the control room areas.

Regular contractors attending the security room(s) will sign a disclaimer that they understand their responsibilities under the General Data Protection Regulations and Human Rights Act – where necessary training will be provided. (Appendix 2)

7. Cameras

OUSS CCTV system provide surveillance opportunities across the University estate and this includes public areas within the immediate vicinity of University buildings. The location and operational requirement of each CCTV camera is reviewed annually as part of the regular audit process, to ensure they are fit for purpose and that there is still a legitimate reason and pressing need for their continued use. (Appendix 3)

The majority of the cameras offer full colour pan, tilt and zoom (PTZ) capability, some of which may automatically switch to monochrome in low light conditions. None of the cameras forming part of the system will be installed in a deliberately covert manner, however, architectural sensitivities and planning restrictions have dictated that some of the system cameras are enclosed within 'all weather domes' or ‘street lanterns’ for aesthetic reasons. The presence of cameras in an area are identified by appropriate signs. (Appendix 4)

All the cameras have pre-set resting positions which are identified by the OM, or nominated person, in response to current and emerging crime trends and intelligence identified by analysing information recorded on the OUSS Command and Control system and intelligence shared at the regular partnership Operation Review Meetings.

CCTV cameras are used to support the OUSS patrol strategy and cameras driven by trained operators are used for general patrol of areas or in response to a focussed tasked area or incident response such as an intruder or fire alarm activation.

8. CCTV signs

CCTV signs advising people that CCTV cameras operated by OUSS are monitoring and recording activity in the immediate area are displayed across the University Estate. The signs indicate:

- The objectives of the CCTV camera system.
- The operator details and contact telephone number.

(Appendix 4)

9. Privacy Issues – Data Protection Impact Assessment (formerly PIA)

The OUSS CCTV system is the subject of a Data Protection Impact Assessment. (Available to view on request)

OUSS CCTV cameras are not positioned or operated in a manner that is likely to cause a disproportionate impact on privacy or any particular community group.

10. Monitoring Equipment

The main control room is located at the Old Observatory, South Parks Road, Oxford. It is staffed 24hrs a day 365 days a year by security officers who are trained to operate any of the system cameras which are active 24 hrs a day. Cameras can also be viewed by trained security officers at the satellite monitoring facility in the security room located at Old Road Campus (ORC).

Third party monitoring of OUSS CCTV cameras is permitted by agreement with departments & colleges. A Memorandum of Understanding between OUSS and the third party is completed to facilitate this arrangement. (Appendix 5)

OUSS have a live link through to Thames Valley Police CCTV suite to facilitate live streaming of incidents from OUSS, this arrangement is facilitated by the existence of an Information Sharing Agreement. (See supporting documents)

11. Orion

The University of Oxford has a specifically designed CCTV IP Control System. It is an open architecture control platform for surveillance applications and it enables seamless control of both traditional analogue and IP security technology.

Security Services manage the University Orion platform from which they can control live video from IP and analogue cameras, retrieve, download and replay recorded video. The OUSS CCTV system operates using the Orion platform. The Orion platform is part of the closed university network system which is maintained by University IT services.

All University departments can utilise the Orion platform for the management of their own CCTV systems and with appropriate authorities OUSS CCTV operators can view, review, replay and download department CCTV cameras.

12. Retaining and processing images

In general recorded CCTV images are retained for a period of no longer than 30 days after which the images are automatically deleted from the system. In exceptional circumstances the OM, or nominated person, can authorise the retention of CCTV images for a longer period of time.

The OM, or nominated person, will ensure the forensic integrity of stored images as this is crucial in providing law enforcement agencies with images of evidential quality, most important is the retention and processing of images and the meta data (ie: time, date and location) which is set by an automated IT system. The current compression of data on the system does not reduce its quality. OUSS systems produce digital images and information that are compatible to the local police requirements.

It is important that individuals and the wider community have confidence that the OUSS CCTV system works efficiently, and is deployed in pursuit of a legitimate reason and to address a pressing need, to protect and support them, and the processes around the handling of personal data is in compliance with the general Data Protection Regulations and processes and procedures are clear and transparent.

The CCTV reviewing suite is located outside the main control room in the secure briefing room, the computer terminal is surveyed by CCTV. Users of the reviewing suite have unique and individual log in details, the systems activities are therefore auditable.

Images required by law enforcement agencies will be downloaded, as per the disclosure guidance, they will then be processed and handed to the appropriate agency who then become responsible for the ongoing management of the images in accordance with the General Data Protection Regulations. OUSS will not retain any copies of the requested images.

13. Disclosure

All requests for disclosure of personal data retained on the OUSS CCTV system will be recorded as a command and control 'incident' log'' and referred to the OM or Duty Manager who will consider the following:

(i) General Data Protection Regulations 2018

Provide for the processing of personal data for law enforcement purposes and includes crime prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security of data.

The requesting organisation must complete the relevant disclosure request form, available at www.admin.ox.ac.uk/ouss/ and deliver this to Security Services for consideration. The following will be considered by the OM or duty manager:

- The information requested is compatible, and will not be used in any way that is not compatible with the stated purpose.
- Non-disclosure would prejudice the stated purpose
- Information given on the form is correct

(ii) Requests for Copies of CCTV images from individuals

Individuals are entitled to requests copies of CCTV images. If they wish to see their own image, the request will be processed as a 'subject access request'. If they wish to see other images, the request will be processed under the Freedom of Information Act (FOIA). Both types of request are handled centrally by the University's Information Compliance Office in the Council Secretariat. There is no requirement for individuals to refer to either piece of legislation when making their request.

Action to be followed by department

If an individual asks the department to provide a copy of a CCTV image, whether orally or in writing, the department will:

A. Record the following information from the individual:

- name and address
- nature of the images requested
- the date and time the images were recorded
- the location of the CCTV camera
- information to identify the individual if necessary

B. Seek to ensure that the relevant images are preserved by making a copy. The OM must be informed that a potential 'subject access request' or Freedom of Information request has been made;

C. Retain the images securely for a period of 12 months; and

D. Ask the individual to contact the University's Information Compliance Office, by emailing data.protection@admin.ox.ac.uk (where the individual wants their own image) or foi@admin.ox.ac.uk (in other cases). If it is unclear what they want, the department will advise them to phone the Information Compliance office on 01865 280299.

(iii) Requests to View CCTV images from individuals

Individuals may wish only to view an image rather than obtain a copy e.g. to check for a lost item of property or to see if there are images of their bike being stolen etc. Such requests should be treated with caution, as the viewing of an image showing other people and would still fall within the scope of the General Data Protection Regulations 2018.

Action to be taken by the department

- Establish clearly why the individual wants to view the image

- If the department is satisfied that the request is being made for a legitimate reason, an authorised member of staff should offer to view the image on behalf of the individual and to inform them of what it shows.

- An individual should only be allowed to view an image themselves where (i) the image does not show other people: and (ii) it can be viewed without gaining access to other images.

- If the image clearly shows other people and the individual insists on seeing the image for themselves, they should be asked to email: foi@admin.ox.ac.uk or to call the Information Compliance Office on 280299

- If they wish to receive a copy of the image, the procedure outlined above should be followed.

14. Partnerships and Information Sharing

OUSS support a number of partnership arrangements designed to further the objectives of the CCTV scheme with organisations such as Thames Valley Police, Oxford Safer Community Partnership, Colleges and Departments. Some of these partnerships involve OUSS viewing images owned by our partners and in these cases all of the safeguards, procedures and standards set out in this policy are applied. Others involve OUSS sharing their images with the partners, in these cases separate Information Sharing Agreements are in place (See supporting documents)

15. Complaints procedure

A member of the public wishing to register a complaint with regard to any aspect of the OUSS CCTV system may do so in writing addressed to:

The Head of Security
The Old Observatory
South Parks Road
Oxford. OX1 3RQ

The Head of Security will ensure that every complaint is acknowledged in writing within a reasonable time period, which will include advice to the complainant of the enquiry procedure to be undertaken. The Head of Security will liaise with the Data Controller and Legal Services. The complainant will be informed in writing the result of the investigation.

16. System Inspections

In the interest of openness and transparency there will be unrestricted access to the CCTV control room to any University personnel nominated to carryout inspections.

The OUSS CCTV Codes of Practise is available to view on the OUSS website.

17. Annual Audit and Report

The OUSS CCTV system will be subjected to an annual audit. The audit will provide an opportunity to review staff training, operators' consultation, CCTV signage, processes and procedures and review every camera position to ensure the cameras are placed in pursuit of a legitimate aim and necessary to meet a pressing need that it is a proportionate response, effective and compliant with relevant legal obligations. (See supporting documents)

An annual report for the OUSS CCTV system will be produced by the OM, or nominated person, and made available to view in the OUSS website. (See supporting documents)

18. Camera Faults

CCTV faults are recorded on the secure OUSS Command and control system and reported to the CCTV maintenance provider on a regular basis by the OM, or nominated member of staff.

19. New cameras

The OUSS Operations Manager, together with the relevant stakeholders, will document the Operation Requirement for any new cameras, ensuring that there is justification, a legitimate reason and a pressing need for each camera. (Appendix 7)

The Operational Requirement document will be signed off by a member of the Crime Reduction team to ensure alternative mitigating measures have been considered and discounted.

New Capital building projects provide an opportunity to deploy additional CCTV cameras in pursuit of the systems objectives. The provision of additional CCTV cameras will be agreed by the Operations Manager and a member of the Crime Prevention Team. The Operational Requirement for these cameras will be subjected to the agreed process above.

20. Deployable camera

OUSS own a deployable CCTV camera intended for use in an overt manner to address ongoing incidents of crime or anti-social behaviour directly affecting University property. The camera records to a pre-loaded SD card which will overwrite every 4 days, it is fitted with a PIR movement sensor to avoid continuous operation when there is no movement.

The deployable CCTV camera can only be deployed with the express authority of the OM and in consultation with the Crime Reduction Team. There must be a legitimate reason and a pressing need to deploy the CCTV camera. The reasons for the CCTV deployment will be recorded and the deployable camera document will be completed (Appendix 8).

CCTV signs must be displayed in close proximity to the camera position.

The decision to deploy the mobile CCTV Camera should be regularly reviewed to ensure that there is a pressing need and legitimate reason for its continued deployment.

21. Maintenance and management

The OUSS CCTV system is subject to an ongoing servicing and maintenance contract. The Operations Manager or nominated person meet regularly with the servicing /maintenance providers to review and progress any long term camera faults or other operating issues.

22. Body worn cameras/Facial recognition/Unmanned Aerial Vehicles/Automatic number plate recognition

OUSS do not have body worn cameras, operate CCTV with facial recognition, automatic number plate recognition functions or operate unmanned aerial vehicles.