Estates Services

# SECURITY SERVICES

UNIVERSITY OF OXFORD

## Code of Practice

Closed Circuit Television (CCTV)

CUSTOMER SERVICE EXCELLENCE CSE

# Contents

Appendices: (available on request to Security Services)

# 1. Introduction

The University of Oxford Security Services (OUSS) 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.

This Code of Practice (the Code) determines best practice in regards to how OUSS operates the CCTV system in accordance with legislative requirements and regulatory guidance.

# 2. Scope of the Code

The Code only applies to CCTV operated and maintained by OUSS
Surveillance devices operated and maintained by divisions, departments, faculties, or other bodies within the university are the responsibility of those bodies. Where this is the case an appropriate policy document or code should be implemented by that body to ensure CCTV systems operate in accordance with legislative requirements and regulatory guidance.

Surveillance devices operated by Colleges or permanent private Halls are not the responsibility of the University. Colleges and Permanent Private Halls are data controllers in their own right and the University hold no responsibility over how they process personal data – including CCTV images[1]
Surveillance devices operated and maintained for research or academic purposes are the responsibility of the researcher or research team who own and /or operate those devices.

# 3. Definitions

The Code will use the following definitions throughout the document:

Data Controller: The 'controller' is defined, by Article 4(7) of the General Data Protection Regulation (GDPR), as a body which alone or jointly determines the purpose and means of the processing of personal data.

For the images produced by the CCTV system the University of Oxford is the controller. The University of Oxford is registered as a data protection fee payer on the Public Register at the Information Commissioners Office. The University's registration number of Z575783X

Data Processor: A data 'processor' is defined, by Article 4(8) of the GDPR, as a body which processes personal data on behalf of a controller.

[1] Kellogg College, Reuben College and St Cross College are established as University societies as opposed to independent colleges or Permanent Private Halls – this is as per Statue V of the University Statues and Regulations. These colleges are therefore considered to be within the scope of the University's remit as data controller. For the purposes of this document these colleges will be considered as 'University bodies' and therefore this Code does not apply to CCTV maintained and operated by these colleges.

**Data Subject:** a data 'subject' is defined, by Article 4(1) of the GDPR, as a living individual who can be identified from personal data. In the case of CCTV a data subject is likely to be an individual whose image has been captured by a CCTV system.

**CCTV System Users:** For the purpose of this document CCTV users will refer to employees who are authorised to use and operate the OUSS CCTV system. Not to be confused with 'The System Operator'

**The Code:** This document (OUSS Code of Practice for CCTV) is referred to as 'the Code'

**The Information Commissioner:** The Information Commissioner is the UK independent regulator whose office (the ICO) upholds information rights – this includes the data protection and privacy aspects of the surveillance.
The ICO have written and published regulatory code of practice in relation to surveillance cameras which this Code takes into consideration.

**The System Operator:** For the purposes of this document the system operator of the CCTV system is Oxford University Security Services (OUSS) and the operational Manager is OUSS Operations Manager. Not to be confused with the 'CCTV System Users'

**The Surveillance Camera Commissioner:** The Surveillance Camera commissioner is a statutory appointment whose statutory functions are to encourage and advise on compliance with the 'Surveillance Camera Code of Practice' (which this Code takes into consideration.
**The University:** This document refers to the Chancellor Masters and Scholars of the University of Oxford (or commonly known as the University of Oxford) as 'the University'

**Third Party:** This document uses the term third party to refer to an individual or body other than the controller, processor or data subject.

**University Bodies:** This document uses the term University Body to refer to a division, department, faculty, school, institution or other entity bound by the University statutes and regulations and therefore within the remit of the University as a data controller.

# 4. 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.

# 5. Legislative and Regulatory Requirements

As the controller for the system, the University is obliged to comply with several legislative texts including, but not necessarily limited to:

- *The General Data Protection Regulations (GDPR) and Data Protection Act 2018 (DPA)*
- *The Freedom of Information Act 2000 (FOA)*
- *Protection of Freedoms Act 2012 (POFA)*
- *Regulation of Investigatory Powers Act 2000 (RIPA)*
- *The Human Rights Act 1998 (HRA)*

## 5.1 GDPR and DPA

The GDPR and DPA are based upon six fundamental data protection principles, the principles are:

1. *Lawful, fair and transparent (personal data shall be processed lawfully, fairly and in a transparent manner)*

*Lawfulness:* As a controller the University must have a lawful basis for the processing of personal data. The processing of static and non-static images, and other associated personal data, through the operation of a CCTV system is necessary for the purposes of the legitimate interests pursued by the University (Article 6 (1) (f) of the GDPR. These legitimate interests are outlined in Section 4 of this Code as system objectives.

In order to balance the reliance on this lawful condition alongside the interests, fundamental rights and freedoms of data subjects, who are subject of the processing, the University has completed a Legitimate Interest's Assessment (LIA) which can be found at Appendix 1 of this Code

*Fairness and transparency:* OUSS meets this requirement achieving voluntary certification with the Surveillance Camera Commissioners Codes of Practice, which sets out a framework for surveillance camera systems to be proportionate and transparent and has also published the following documents:

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

2. *Purpose limitation (personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes)*

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

3. *Data minimisation (personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose of the processing*

OUSS meets this requirement by carrying our annual audits to review the positioning of individual cameras, in relation to the objectives, to ensure that cameras only capture images of the intended area and does not capture images of areas outside of scope or areas which could cause privacy concerns (e.g. ensuing cameras do not capture private properties).
OUSS also operates strict restriction processes to ensure that only authorised individuals have access to CCTV systems and personal data captured by that system.

*4. Accuracy (personal data shall be accurate, and where necessary kept 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 (personal data shall be kept for no longer than is necessary for the purposes for which it is processed).*

OUSS meets this requirement by ensuring that the routine retention of recorded material does not exceed 30 days unless there is a valid, justified and lawful purpose to retain the data for an extended period of time - for example where the personal data is required for the or defence of legal claims.

*6. Security (personal data shall be processed in a manner that ensures appropriate security of those data*

OUSS meet this requirement by formulating and implementing appropriate technical and organisational policies and procedures.
The GDPR and DPA also include a further 'accountability' principle. This principle obliges data controllers to demonstrate compliance with the above principles. This code together with the DPIA and annual audit fulfils this requirement
The ICO have prepared and published a surveillance camera code of practice to encourage all organisations, who operate surveillance systems, to ensure those systems adhere to the above principles. The University has taken that regulatory code into account when writing this University Code and when completing its annual DPIA review.
The provisions of the GDPR also allows individuals to request CCTV images. Details about how the University manages such request can be found in section 15 of this Code.

## 5.2 FOIA

The University is a public authority for the purposes of the FOIA. This requires the University to publish certain information including how an organisation operates, how it spends money and what policies and procedures it maintains – this is known as a publication scheme and is intended to encourage open access to information. The University includes information about its centrally managed CCTV system, within this publication scheme, through the publications of this code and the publications of its annually reviewed data protection impact assessment.
The provisions of the FOIA also allows individual to request CCTV images. Details about how the University manages such requests can be found in section 15 of this Code.

## 5.3 Surveillance Camera Code of Practice 2013

The POFA sets out a provision that the Secretary of State for the Home Department will prepare and publish a Surveillance Code of Practice that will be promoted and reviewed by the Surveillance Camera Commissioner.
The Code sets out 12 guiding principles that apply to 'relevant authorities'. The University of Oxford is not defined within the POFA as a relevant authority and as such are not obliged to implement that Code. However, OUSS has achieved voluntary certification with the Surveillance Camera Code of Practice.

The surveillance camera code of practice obliges that surveillance camera systems in public places, operated by relevant authorities, are designed to provide a framework for operators and users of surveillance camera systems to define 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)*

## 5.4 RIPA

RIPA is concerned with 'the monitoring, observing or listening to persons, their movements, conversations, or other activities and communications….carried out in a manner calculated to ensure that any persons who are subject to the surveillance is unaware that it is or may be taking place' i.e. Covert surveillance activity[2]

The Act states that any legal body undertaking covert surveillance activity must be authorised to do so by schedule 1 of RIPA. The University is not authorised, by this schedule, to undertake covert surveillance activity.

## 5.5 HRA

The University recognises that the relevant authorities and those organisations carrying out the functions of a public service nature are required to observe the obligations imposed by the HRA, and consider that the use of CCTV across the University precincts is necessary, addresses a legitimate aim and justifiable 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 a use of 'operational requirements' 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 to individuals. It is recognised that the operation of the CCTV system may be considered to infringe on privacy of the individuals. The University recognises its 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 system's objectives. The University adheres to this principle through the regular conduct of audits of individual cameras, the CCTV System and the CCTV privacy framework.

# 6. CCTV Users

All OUSS CCTV users and authorised staff, including managers, have received training relevant to their role in relation to the above listed legislative texts and regulatory guidance. User training will be subject to an annual audit and refresher training delivered by the internal trainer. Audit and training records will be maintained by the Operations Manager.

OUSS CCTV users have a unique user name and password that has to be entered correctly into the CCTV operating system before they can operate the cameras. This allows OUSS CCTV to maintain audit trails of user access.

OUSS CCTV users are not required to be Security Industry Authority (SIA) licensed because they are employed directly by the University.

[2] Covert surveillance and Property Interference, Revised Code and Practice, Home Office (August 2018)

# 7. Discipline

CCTV operating processes and procedures are available for staff to consult, and are reiterated at CCTV user training and CCTV user refresher training. The documents are available to view on the OUSS operational pages held centrally on the secure Command and control computerised system.

All OUSS 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 2). Such records are maintained by the Operations Manager

Disciplinary action will be taken if a CCTV operator breaches local or legal operating requirements. The Operations Manager is responsible for facilitating disciplinary action and this will be in line with relevant HR processes and policies.

# 8. 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. These arrangements are overseen by the Operation Manager and records are retained and audited by the Operations Manager

Regular contractors attending the security room(s) will sign a disclaimer that they understand their responsibilities under the General Data Protection Regulation and Human Rights Act – where necessary training will be provided. (Appendix 3). All contractors will be subject to a signed contract, which includes statutory data protection clauses, which will be agreed prior to a contracts access to the security room(s). Contracts will be maintained by the Operations Manager

9. 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 that they are fit for purpose and that there is still a legitimate reason and pressing need for their continued use. (Appendix 4) The annual audit process is overseen by the Operations Manager and records maintained by the Operations Manager.

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 5)

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. Detailed meeting minutes record all decisions made at these meetings. These minutes are maintained by the Operations Manager

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.

# 10. CCTV signs (Appendix 5)

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 system operator details and contact telephone number.*

The annual audit of individual CCTV cameras include an assessment that CCTV signs are in good condition and positioned in a clear and visible location.

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

The OUSS CCTV system is the subject of a Data Protection Impact Assessment (DPIA). The University uses the Surveillance Camera Commissioner's template DPIA which has been approved by the ICO. The DPIA is reviewed annually by The Operations Manager and in consultation with the University's information compliance team and other relevant stakeholders.

The updated DPIA is published online alongside this Code for the purposes of transparency.

The outcome of the DPIA ensures that OUSS cameras are not positioned or operated in a manner that is likely to cause a disproportionate impact on the privacy of individuals or any particular community group.

# 12. 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).

University departments monitoring OUSS CCTV cameras is permitted by agreement with those departments. A Memorandum of Understanding (MOU) between OUSS and the third party is completed to facilitate this arrangement. These MOU's are regularly reviewed by the Operations Manager

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.

# 13. 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 users can view, review, replay and download department CCTV cameras. Such arrangements are documented with a MOU which are periodically reviewed. These MOU's are maintained by the Operations Manager.

# 14. 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, where there is a justified , proportionate, and legally compliant purpose to do so – for example in order to exercise or defend against legal claims. Decisions to retain information beyond the standard retention period will be in writing and retained by Operations Manager

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 (i.e. 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 Regulation 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 Regulation. OUSS will not retain any copies of the requested images, unless compelled to do so by other legislative requirements.

# 15. Disclosure and Information Sharing

OUSS maintains processes to handle requests for CCTV static and non-static images from the University bodies, colleges and permanent private halls, individuals (in a personal capacity), law enforcement agencies and other third party organisations.

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 .

## 15.1 Requests from University Bodies

Requests received from other University bodies will not automatically be accepted. Where a University body wishes to access CCTV data then they must make a request in writing clearly stating their intended purpose and why that purpose will be hindered without the access to the CCTV data. The University body must also state their intended lawful basis for processing that data.

The OM or Duty Manager are responsible for accepting or denying requests from other University bodies. The OM or Duty Manager may correspond with the Information Compliance Team to determine the appropriateness of such a request.

All decisions in regards to requests from University bodies will be maintained by the Operations Manager.

The requesting University body will be responsible for ensuring that their handling of that received data is compliant with the data protection principles – notably the second (purpose limitation), fifth (retention) and sixth (security) principles.

## 15.2 Requests from Colleges and Permanent Private Halls

For the purposes of data protection legislation Colleges and permanent private halls are considered to be data controllers in their own right. Whilst the University maintains an overarching information sharing agreement, with each of the colleges and permanent private halls, this agreement does not specifically address CCTV processing and therefore Colleges and permanent private halls must follow the same process detailed at 15.5 of this Code – exception may be given where the University and the College or permanent private hall share a common purpose (i.e. Security of shared property).

## 15.3 Requests from Individuals (in a personal capacity)

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' (SAR) under the GDPR. If they wish to see other images, the request will be processed as a Freedom of Information Request (FOI) under the FOIA.

Both types of request are handled centrally by the University's Information Compliance Team in the University's assurance directorate. There is no requirement for individuals to refer to either piece of legislation when making their request. Information about how to submit a request can be found on the Information Compliance Team's web pages.

All individual requests for information will have consideration for other individuals or personal data captured within the images. Images will be appropriately and securely redacted (through image distortion) where required. Where an image is distorted then the ICT will retain an undistorted copy of the footage for the purposes of auditing decisions made in relation to the request.

## 15.4 Law Enforcement Agencies

A request for CCTV footage, where individuals can be identified (directly or indirectly) from that footage, from law enforcement agencies is likely to be, but not necessarily, requested under schedule 2, part 2, section 1 of the DPA where the purpose of the request is for:

(a) the prevention or detection of crime,
(b) the apprehension or prosecution of offenders, or
(c) the assessment or collection of a tax or duty.

The University maintains an Information Sharing Agreement with Thames Valley Police (TVP). Requests for information made under this agreement must be in writing and using the prescribed documentation at Appendix B of that agreement.

Requests from other law enforcement agencies must be in writing and preferably using the CCTV request form which can be found at Appendix 6 of this Code. Requests must clearly state the intended purpose, why that purpose will be hindered without the access to the CCTV data, state their intended lawful basis for processing that data, and what lawful basis or exemption they're requesting the data under.

The OM or Duty Manager are responsible for accepting or denying requests from Law Enforcement agencies. The OM or Duty Manager may correspond with the Information Compliance Team to determine the appropriateness of such a request.

All decisions in regards to requests from law enforcement agencies will be overseen by the Operations Manager.

## 15.5 Other Third Party Organisations

Requests from other third party organisations must be in writing and preferably using the CCTV request form which can be found at Appendix 6 of this Code. Requests must clearly state the intended purpose, why that purpose will be hindered without the access to the CCTV data, state their intended lawful basis for processing that data, and what lawful basis or exemption they're requesting the data under.

The OM or Duty Manager are responsible for accepting or denying requests from other third party organisations. The OM or Duty Manager may correspond with the Information Compliance Team to determine the appropriateness of such a request.

## 15.6. Requests to View Footage

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 GDPR.

Where such a request is received then OUSS will:

- *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, then their request should be passed on to the information compliance team so that the correct procedure can be followed (see 15.3 above)*

## 15.7 Emergency Requests

It is appreciated that in some emergency situations access to CCTV footage may be required urgently and the proper process outlined above may be disproportionately burdensome for the situation – for example in a life of death scenario where CCTV footage is required to protect an individual's vital interests.

Emergency requests will require the authorisation of the OM or Duty Manager. All decisions made will be recorded in writing and all relevant paperwork will be completed retrospectively. The authorising manager will be confident that the purpose of the request is truly to protect and individual's vital interests.

# 16. 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 may liaise with the Information Compliance Team and Legal Services Office. The complainant will be informed in writing the result of the investigation.

Complaints regarding data protection should be made to the information compliance team by writing to:

Information Compliance Team
University of Oxford
University Offices, Wellington Square
Oxford. OX1 2JD
data.protection@admin.ox.ac.uk

# 17. System Inspections

In the interest of openness and transparency there will be unrestricted access to the CCTV control rooms to any University personnel authorised to conduct inspections and/or audits. Authorised personnel will be accompanied by an OUSS staff member at all times. Access to the CCTV control rooms are logged by accompanying OUSS personnel. This log is maintained by the Operations Manager.

The OUSS CCTV Code of Practice is available to inspect on the OUSS website.

# 18. Annual Audit and Report

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

# 19. Camera Faults

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

# 20. New Cameras

The OUSS Operations Manager, together with the relevant stakeholders, will document the Operational Requirement for any new cameras, ensuring that there is justification, a legitimate reason and a justifiable 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 or implemented.

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 subject to the agreed process above.

The deployment of new CCTV systems, or major amendments to existing systems, will require the completion of a Data Protection Impact Assessment (DPIA). The OUSS will liaise with the information compliance team where this is the case.

# 21. 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 passive infrared sensor (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 justifiable 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). These decisions are maintained by the Operations Manager.

CCTV signs must be displayed in close proximity to the camera position so that all individuals captured by the deployable camera are aware of its use.

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

# 22. 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.

All servicing and maintenance providers will be subject to an agreed contract which will contain statutory data protection clauses within. This ensures that any personal data handled by those providers, in order to complete their task, will be done so securely and in accordance with legislative requirements.

# 24. Other Surveillance Devices

OUSS do not operate a CCTV system with facial recognition, automatic number plate recognition (ANPR) devices, unmanned aerial vehicles or body worn cameras.

## ESTATES SERVICES

T: +44(0)1865 2 72944
E: securityservices.updates@admin.ox.ac.uk
estates.admin.ox.ac.uk/security-services

UNIVERSITY OF
OXFORD