CCTV Code of Practice

Oxford Brookes University

v. 1.3
August 2017

Document Control Information:

Document Name:	***CCTV Code of Practice – Oxford Brookes University***
Directorate:	Directorate of Estates and Facilities
Department:	Facilities Services
Document Owner:	Headington Site Manager (Monika Graham)
Deputy Document Owner:	Information Compliance Manager (Sol Khan)
Authorised by:	Director of Estates and Facilities Deputy Director Commercial and Facilities Deputy Director Estates Head of Information Management
Signed:	…….. (Director of Estates and Facilities) …….. (Deputy Director – Facilities and Commercial Services) …….. (Deputy Director - Estates) …….. (Head of Information Management)
Date Authorised:	
Review Date:	February 2018

Version Control

Version	**Date**	**Summary of changes**
1.0	01/05/2015	Revised draft
1.1	1/06/2016	Changes to titles of responsible persons
1.2	18/05/2017	• Further changes to the titles of responsible persons • Clarification of the objectives of CCTV system and the release of recorded material • Full review of the content • Frequency of review
1.3	01/08/2017	• Sign off by HR Department and Unison

Contents:

1. Definitions used in this Code of Practice

The System: A Closed Circuit Television (CCTV) System in use at Oxford Brookes University and operated from 24/7 Control Room

Data Controller: Oxford Brookes University

System Owner: Director of Estates and Facilities Management

System Manager: Deputy Director Commercial and Facilities or delegated representative (see Appendix 1 for detailed list)

System Maintenance: Building Controls and Systems Manager, Estates Division

System Operator: Security Manager, MITIE Security

2. Oxford Brookes University Statement in respect of The Human Rights Act 1998

Oxford Brookes University recognise that public 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. Oxford Brookes University considers that the use of CCTV in the campuses is a necessary, proportionate and suitable tool to aid the prevention and detection of crime and assist to identify offenders.

The Oxford Brookes University CCTV System shall be operated with respect for all individuals, recognising the right to be free from inhumane or degrading treatment and avoiding discrimination on any ground. Further the System shall be operated in such a way as to avoid infringement of individual privacy in normal operation.

Oxford Brookes University recognises that it is their responsibility to ensure that the system should comply with all relevant legislation, to ensure its legality and legitimacy. The system will only be used as a proportional response to incidents.

3. Objectives of the CCTV System

The Objectives of the CCTV systems are to reduce crime and the fear of crime by helping to provide a safer environment for those people who study, visit and work in the University.

The system will provide the University and Police with assistance to detect, deter and prevent crime. It will:

- help identify, apprehend and prosecute offenders
- provide the Police with evidence to enable criminal and civil proceedings to be brought through the legal system
- enable, as far as is reasonably practicable, a safe environment for students, staff and visitors
- investigate incidents where conduct of staff and students has not been in line with University policy.

The system will be operated at all times with due regard for the privacy of individuals.

Any user found to have unlawfully compromised the privacy of individuals in breach of this Code of Practice, will be subject to the disciplinary procedures of Oxford Brookes University and may be reported to the authorities. Non-compliance of third parties will be subject to contractual penalties or may face criminal charges by the authorities.

The key objectives of the system are:

- to provide public reassurance and to deter crime
- to improve general security in the area, both in terms of personal safety and the security of buildings and premises
- to assist the Police with specific operations
- to protect Oxford Brookes University from spurious claims of negligence
- to assist with the surveying of the premises to ensure the property is maintained in good order
- to enable Oxford Brookes University to investigate incidents
- to facilitate the identification of inappropriate activities and the collection of evidence to support disciplinary proceedings in relation to staff or students.

Disclosure of recorded material will only be made to third parties in strict accordance with the objectives of the system and the Data Protection Act 1998.

4. Statement of Purpose & Principles of the CCTV Code of Practice

4.1 Purpose

The purpose of this document is to state how the owners and managers, on behalf of Oxford Brookes University intend to use the Oxford Brookes University CCTV System (hereafter referred to as 'The System') to meet the objectives and principles outlined in section 3.

4.2 General Principles of Operation

1. The System will operate under all applicable legislation passed by EU, UK and English law.
2. The system will be operated in accordance with the Data Protection Act 1998 at all times. All personal data processed by using the system will be in accordance with the principles of the Data Protection Act 1998. Personal data must be:

- processed fairly and lawfully
- processed only for one or more specified and lawful purpose
- adequate, relevant and not excessive
- accurate and kept up to date
- kept for no longer than is necessary for the purposes it is being processed
- processed in line with the rights of individuals
- secured against accidental loss, destruction or damage and against unauthorised or unlawful processing
- not transferred to countries outside the European Economic Area.

3. Participation in the system by any 3rd party organisation, individual or authority will be on condition that all parties agree to comply fully with this code and to be accountable under the Code of Practice.
4. Copyright and ownership of all material recorded by virtue of the system will remain with the University who will act as the Data Controller.
5. The Buildings Controls and Systems Manager is to maintain an up to date inventory of all camera locations.
6. The system uses a digital operational recording facility securely located throughout the University. A copy of the list of recording facilities is kept securely in the Control Room. Those operating or downloading CCTV will be authorised by the Deputy Director Commercial and Facilities or his representative to do so.
7. No recorded material, whether recorded digitally, in analogue format or as a hard copy video print, will be released from the Control Room unless it is in accordance with this Code of Practice. A CCTV data release log will be kept up to date for audit trail purposes.
8. This Code of Practice will be subject to periodic review every year or following any major security incidents to ensure that it reflects best practice and responds to legal requirements.

9. Strategic responsibility for security management rests with the Deputy Director Commercial and Facilities, with day-to-day operational management delegated to Site Managers.

10. All breaches or near misses of the Code of Practice must be reported to Oxford Brookes University's Information Compliance Manager or his representative and he/she shall have responsibility for investigating and managing all breaches. Information Security Incident Management Policy can be found here: www.brookes.ac.uk/it/information-management.

11. Any request from an individual for the disclosure of personal data, which he/she believes is recorded by virtue of the System will be directed in the first instance to the Information Management Team (info.sec@brookes.ac.uk).

12. The University's Data Protection Policy can be found here: www.brookes.ac.uk/it/information-management/policies-procedures-legislation.

13. University Guidance on the Freedom of Information Act can be found here: http://www.brookes.ac.uk/it/information-management/foi/

5. CCTV Operation

5.1 CCTV Monitoring

CCTV monitoring operators will not be permitted to use the CCTV system until they have received suitable training and are familiar with this Code of Practice.

Where a control centre requires operators to be licensed, in accordance with the law, no staff may operate cameras subject to the legislation without a Public Space Surveillance (CCTV) licence.

Every person involved in the management and operation of the System will be personally issued with a copy of the Code of Practice. They will be required to sign confirmation that they fully understand their obligations to adhere to this policy and the consequences of any breach. This Code will be updated from time to time, and CCTV operations will be informed of the changes.

A list of authorised persons to monitor and download CCTV images will be kept up to date by the System Manager and reviewed annually. All requests for download of CCTV should be authorised by the System Manager.

5.2 Declaration of Confidentiality

Every individual with responsibility under the terms of this Code of Practice and who has any involvement will be required to sign a declaration of confidentiality (see appendix 2).

5.3 Control and Operation of Cameras

Cameras will not be used to look into private residential properties, unless it is necessary for the purpose of prevention and detection of crime and the apprehension of offenders.

To ensure compliance with the Information Commissioners Office (ICO) CCTV Code of Practice and that images recorded continue to be of appropriate evidential quality, Oxford Brookes University CCTV

System shall be maintained by the University's Building Controls and Systems Department.

The maintenance programme will make provision for regular/periodic service checks on the equipment which will include cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment, which is reaching the end of its serviceable life.

5.4 Access Arrangements and Security of Central Control Room

Access and security arrangements to central Control Room shall as a minimum comply with the following:

- Access to the Control Room is strictly controlled and only those persons on legitimate business are allowed access.
- A detailed record will be maintained of visitors to the control room and access is only allowed after formal identification has taken place.
- Access for visitors to view the system will only be permitted by the authorisation processes described above.
- A logbook of visits to the control room is maintained. This book contains details of the individual and organisation, date, time and purpose of visit.
- All works to the control room will be carried out in strict compliance with current Health and Safety requirements and in accordance with accepted best practice.

5.5 Management of Recorded Material

For the purposes of this Code 'recorded material' means any material recorded by, or as the result of, technical equipment, which forms part of The System, but specifically includes images recorded digitally.

The management of recorded evidence will be compliant with ICO CCTV Code of Practice, which can be found here: https://ico.org.uk/media/fororganisations/documents/1542/cctv-code-of-practice.pdf

Any images obtained from the System must be treated strictly in accordance with this Code of Practice from the moment they are received by the Control Room until final destruction. All transfers of data must be recorded. Access to and the use of recorded material will be strictly for the purposes defined in this Code of Practice.
Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment or otherwise made available for any use incompatible with this Code of Practice.

Information will be made available for traffic and transport monitoring, management and information purposes.

5.6 Retention of Recorded Material

CCTV images will be retained on re-usable media for one month. Before reuse or destruction, media will be erased in full accordance with the manufacturer's requirements. Digital recording will be set to

overwrite automatically. At the conclusion of their life-span recorded material used within the CCTV System will be destroyed responsibly.

Each discrete item of recorded material (CD, DVD, USB stick etc.) will be registered and monitored from the time it is produced, until it is destroyed, whilst it is within the Control Room. Recorded material will be retained for 1 month from its creation unless an incident is involved, then 6 months from the end of incident, after which it will be destroyed.

If recorded material is released in accordance with this code, a record must be kept which identifies the basis for that release, and to whom. Records will be retained for at least three years.

For the purposes of prevention and detection of crime a section 29-35 notice form must be completed and returned to the Information Compliance Manager, who will process it under the Data Protection Act. If the data is required to protect the vital interests of individuals the System Manager will make a decision based on the nature, purpose and proportionality of the request on whether to release the data. The section 29-35 form can be completed retrospectively.

Appendix 1 - List of responsible System Managers

1. Deputy Director Commercial and Facilities
2. Site Manager – Headington
3. Site Manager – Harcourt Hill and Wheatley
4. Information Compliance Manager

Contact details of the responsible “System Managers” can be found here:

http://www.brookes.ac.uk/estates/facilities-services/

Appendix 2 – Declaration of Confidentiality

I confirm that my employer [name of employer] has provided me with appropriate information security awareness training consummate to my position. I have been made aware of my potential personal liability and implications for my employer from my negligent or malicious actions when processing data on behalf of the University.

I have familiarised myself with the following policies:
Name of appropriate OBU Policy

I have undertaken the following information security awareness training programmes:
Date / title of programme / training provider

I warrant to Oxford Brookes University that the above information is true and accurate to the best of my knowledge and belief.

Name:
Signature:

I confirm to the best of my knowledge and belief and the above member of staff has had the appropriate training and qualifications to perform the role of *[Enter Role]*.

Name on behalf of *[name of employer*]:
Signature on behalf of *[name of employer]:*

Appendix 3 – Internal CCTV Data Download Request Form*

*This form should be completed to facilitate the identification of activities and the collection of evidence, which might warrant disciplinary proceedings being taken against staff or students

1. Requester

First name(s):	Last name:
Job title:	Faculty / Directorate:
Email:	Telephone:

2. Specific information required

Date and time of incident (please use 24 hr clock or mark am/pm): Exact location: Description of incident / Reason for Request:

3. Data subject (if applicable)

First name(s):	Last name:
Address: Other identifying information:	

4. Information provision

If we hold information how would you like the information to be provided?

☐ Electronically using encrypted documents (sent via email with decryption passwords relayed by telephone call)

☐ Collect in person (proof of identification required when collecting)

5. Declaration and authorisation

I certify that:

- I understand information given on this form is correct
- I understand that if any information given on this form is incorrect I may be committing an offence under Section 55 of the Data Protection Act, 1998

Signed:	Date:

6. Authorising line manager*

*this must be a Directorate/Faculty representative in a sufficiently senior position to authorise this request, normally at a Director's or Dean's level

First name(s):	Last name:
Job title:	Faculty / Directorate:
Email:	Telephone:

Where to send your request

Please note: If the form has not been fully or properly completed and authorised you will be asked to re-submit your application. Send this form to:

Encrypted Email*:

If you have a PSN approved encrypted mail system, please send your completed form to:

info.sec@brookes.cjsm.net

Postal address:

Information Compliance Officer Oxford Brookes University Oxford Brookes Information Systems (OBIS) Room 2.12 Gibbs Building Headington Campus Gipsy Lane Oxford OX3 0BP

Fax: We do not accept faxes

Oxford Brookes University Use Only

Release Authorisation Information approved for release:

Yes □ No □

First name(s):	Last name:
Job title:	Faculty / Directorate:
Email:	Telephone:

Appendix 4 – Section 29-35 Disclosure Request Form (Data Protection Act)

1. Requestor

First name(s):		Last name:
Job title:		
Organisation:		
Address:		
Postcode:		Telephone:
Email:		

2. Data subject

Current details

First name(s):	Last name:
Address:	

Other identifying information

3. Specific information required

4. Reason for requesting disclosure

Offence(s) or suspected offence(s)

☐ **Unable to specify offence due to risk of prejudicing the case**

Statutory powers (Do not cite section 29/35 of the Data Protection Act)

Purpose

State the purpose for requesting disclosure of personal information about the data subject specified in section 2 of this form.

Select one option

☐ Prevention or detection of crime

☐ Apprehension or [prosecution of offenders

☐ Assessment or collection of tax, duty or imposition of a similar nature

☐ For the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)

☐ For the purpose of obtaining legal advice

5. Information provision

If we hold information how would you like the information to be provided?

☐ Electronically using encrypted documents (sent via email with decryption passwords relayed by telephone call)

☐ Collect in person (proof of identification required when collecting)

We will notify you if we do not hold information or your request for disclosure is refused

6. Declaration and authorisation

The authorising officer must be of the rank of police inspector or higher, or for other 'relevant bodies' a senior officer/manger.

Declaration

I certify that:

☐ Information requested is compatible with the stated purpose (section 4) and will not be used in anyway incompatible with that purpose

☐ Non-disclosure would prejudice the case

☐ I understand information given on this form is correct

☐ I understand that if any information given on this form is incorrect, I may be committing an offence under Section 55 of the Data Protection Act, 1998

Requestor

Signed:	Date:

Authorising Officer (Requesting Organisation)*

*this must be an officer of the organisation, in a sufficiently senior position to authorise this request

First name(s):		Last name:
Job title:		
Signed:		Date:

Where to send your request

Please note: If the form has not been fully or properly completed and authorised you will be asked to re-submit your application.

Send this form to:

Encrypted Email*:

If you have a PSN approved encrypted mail system, please send your completed form to:
info.sec@brookes.cjsm.net

Postal address:

Information Compliance Officer
Oxford Brookes University
Oxford Brookes Information Systems (OBIS)
Room 2.12
Gibbs Building
Headington Campus
Gipsy Lane
Oxford
OX3 0BP

Fax: We do not accept faxes

Oxford Brookes University Use Only

Release Authorisation Information approved for release:

Yes □ No □

First name(s):		Last name:
Job title:		
Signed:		Date: