OXFORD BROOKES UNIVERSITY

Closed Circuit Television (CCTV) and Body Worn Video (BWV) Policy (the Policy)

Document Control Information:

Document Name:	Closed Circuit Television (CCTV) and Body Worn Video (BWV) Policy
Directorate:	Directorate of Estates and Campus Services
Department:	Campus Services
Document Owner:	Head of Campus Services (Monika Graham)
Deputy Document Owner:	Head of Information Security Management (Gareth Packham)
Approvals required:	Director of Estates and Campus Services Head of Campus Services Campus Director Director of Estates Head of Information Security Management
Signed:	M. Graham ..... (Head of Campus Services) ..... (Deputy Director Commercial and Campus Services) .....Jerry Woods..... (Director of Estates and Campus Services) ..... (Head of Information Security Management) ..... (Job Title) on Behalf of Security Services contractor
Date of Approval:	[October 2020]
Renewal date and responsibilities:	Annually by the Information Security Working Group or following any major security incidents or at the instigation of the Head of Information Security Management (whichever is the earlier date).

1. Definitions

Body Worn Video BWV: wearable body camera equipment which records audio, video, or photographic material as required. Any BWV used will allow for images and voice to be recorded and downloaded.

Data Controller: in this instance Oxford Brookes University (the "University") as defined in Article 4 General Data Protection Regulation and as amended.

Data Subject: as defined in Article 4 General Data Protection Regulation and as amended. In this instance, individual being recorded.

Personal Data as defined in Article 4 General Data Protection Regulation is any information (including a recording) which relates to an identified or identifiable individual and it may include image and voice.

Pixelation or blurring of an image is a technique used to obscure a person's face or identifying features so as to render them unidentifiable as a particular individual. This is to protect their privacy rights.

Recorded material: any material recorded by, or as the result of, technical equipment, which forms part of the CCTV System, or is recorded by the BWV.

System Maintenance: Building Controls and Systems Manager, Estates Division

System Manager: Head of Campus Services or delegated representative (see Appendix 1

for detailed list)

System Operator: Contracted Security Services

System Owner: (of the CCTV System) Director of Estates and Campus Services/Head of Campus Services

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

2. Context and application of the Policy

2.1 This Policy applies to all parties who seek to rely on CCTV or BWV footage recorded on premises used by the University.

2.2 It sets out how CCTV and BWV footage may be used within Oxford Brookes University. It explains when footage may be shared lawfully within the University and externally with third parties.

2.3 The System will be operated at all times and any BWV footage will be recorded with due regard for the privacy of individuals being recorded (the Data Subjects).

3. The Reasons that Oxford Brookes has a CCTV System and why BWV equipment may be worn

These security measures are available to:

- reassure those on the University premises that in the event of an incident, CCTV or possibly BWV footage may be available to support any subsequent investigation
- act as a deterrent to any such incidents happening and so contribute to a safe environment
- help to identify, apprehend and prosecute or sanction offenders. Footage may provide the police and others with supporting evidence to enable criminal and civil proceedings to be brought through the legal system (including where specific police operations are underway)
- be used to support the investigation of incidents where conduct of staff, students or others has not been in line with: University policy, regulations or their contract of employment, or where there is otherwise apparently unacceptable behaviour, or are contrary to law or Government Guidelines (this is particularly relevant but not restricted to the pandemic)
- be relied upon by the University in negligence proceedings, where there is a recording of an accident or other incident, for example
- be used to ensure that the University premises are in good order
- be used for traffic monitoring
- be used to support an investigation which is not directly relevant to the University save it may have been recorded on or close to University premises
- be used to support Data Protection Subject Rights Requests (including access)

- to support investigations or enquiries carried out by relevant stakeholders (such as contractors or other employers working on site) with a view to achieving these same aims
- any other purpose which is broadly equivalent to these aims, as determined by the Head of Information Security Management

4. Statement of Purpose & Principles of the CCTV and BWV Policy

4.1 Purpose

The purpose of this Policy is to set out how CCTV recordings and BWV will be used within Oxford Brookes University: to meet the objectives and principles outlined in sections 3 and 4 Forms are available in the appendices which are to be completed to document the release of information.

4.2 Principles of operation of CCTV and BWV:

CCTV

4.2.1 The CCTV system will operate in accordance with any applicable legislation, Guidance, Regulations Codes of Practice or Conduct and relevant Policies.

4.2.2 There must be signage highlighting clearly and visibly that CCTV is in use.

4.2.3 The CCTV 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 Campus Director or his representative to do so.

4.2.4 The Security Manager (on behalf of the Security Services contractor) is to maintain an up-to-date inventory of all camera locations (CCTV) and a list of those trained in their use (both CCTV and BWVs), which can be reviewed by the Head of Information Security Management or delegated nominee.

Generally:

4.2.5 Strategic responsibility for security management rests with the Campus Director, with day-to-day operational management delegated to Campus Managers.

4.2.6 Recognisable images of people and recordings constitute Personal Data, as prescribed in Data Protection law. Personal Data must be processed with due regard to the Principles in Ss 86-91 Data Protection Act 2018 that require that processing must be (as paraphrased here):

- lawful, fair and transparent
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and where necessary kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed
- processed in a manner that ensures appropriate security of the personal data

- destroyed in accordance with the University requirements (in the Brookes retention schedule)

4.2.7 Copyright and ownership of any footage will remain with the University being the Data Controller.

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

4.2.9 All breaches of information security or technical assurance or near misses involving the processing of personal data involving BWV equipment or CCTV must be reported to Oxford Brookes University's IT Services Information Security Management team via ServiceNow or by emailing info.sec@brookes.ac.uk. Any incidents must be investigated in accordance with the Information Security Incident Management Policy found here: https://www.brookes.ac.uk/it/information-security/

5. CCTV System Use and BWV Operation

5.1.1 Every person involved in the management and operation of either CCTV or BWV must be provided with access to this Policy by their line manager.

5.1.2 No member of staff may use any of the equipment until they have received suitable training and they are familiar with this Policy and other relevant requirements brought to their attention by their Manager.

5.1.3 Members of the University Security Services team who are involved with the monitoring and provision and use of any footage by whatever means are doing so in accordance with the requirements of any explicit or implied terms relating to confidentiality in their contract of employment. They are required to sign the Declaration of Confidentiality (Appendix 2) confirming that they have received suitable training; that they are aware of their responsibility under the terms of this Policy as well as their contract. This Declaration must be retained by their line manager and be available on request. These staff are bound by any implied or explicit contractual obligations to keep information confidential.

5.1. 4 Any CCTV or BWV user found to have unlawfully, wilfully or negligently unacceptably compromised the privacy of individuals in breach of this Policy may be subject to the disciplinary procedures of Oxford Brookes University, their employer and may be reported to the authorities (e.g. the Police or appropriate regulator). Non-compliance by third parties will be subject to contractual penalties or may face criminal charges by the authorities or other appropriate sanction. Nothing in this Policy should inhibit lawful whistleblowing which is carried out in accordance with relevant procedures.

5.1.5 A list of authorised persons to monitor and download CCTV or BWV images will be kept up-to-date by the System Manager and the System Manager will review it annually to make sure it is up-to-date.

5.1.6 No recorded CCTV or BWV 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 Policy and the pre requisite authority to release has been secured save in an emergency (see Appendix 3).

5.1.7 A CCTV and BWV data release log or logs will be kept up-to-date by the contracted Security Services for audit trail purposes.

5.1.8 Where a person seeks to exercise their Data Subject Rights (see Ss 45-50 Data Protection Act 2018) such as seek a copy of footage which records themselves, the Data Subject should contact the IT Services Information Security Management Team via info.sec@brookes.ac.uk. If the request is received by a third party (such as the contracted Security Services), any request should be forwarded promptly so that it can be dealt within the legal time limit.

5.1.9 Where a control centre requires operators to be licensed, in accordance with the law, no member of staff may operate cameras subject to the legislation without a Public Space Surveillance (CCTV) licence. It is for the University Security Services team to ensure that it is current and valid.

5.1.10 Oxford Brookes University CCTV System shall be maintained by the Security Services contractor to ensure compliance with the Information Commissioner's Office (ICO) CCTV Code of Practice and that images recorded continue to be of appropriate evidential quality. 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.

5.2 BWV Operation

5.2.1 Any BWV worn must be to the security specification as to be agreed by the Head of Information Security Management.

5.2.2 BWV may only be worn and used by suitably trained designated staff.

5.2.3 The BWV user will declare that they are recording as they respond to an incident, with a view to highlighting that recording is going on to all who are present. The BWV user must wear clothing that displays that the wearer is using this equipment. Recording must not be covert.

5.3 Privacy Notices

The Contracted Security Services and the University will ensure that the use of the BWV and CCTV is noted on Privacy Notices.

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 CCTV and BWV Material

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

5.6.2 Any images obtained from the System must be treated in accordance with this Policy and the Code of Practice from the moment they are received by the Control Room until final destruction. All transfers of data must be evidenced in the appropriate log. Access to and the use of recorded material will be strictly for the purposes defined in this Policy.

5.6.3 All requests for download of CCTV or BWV footage should be authorised by the System Manager. Where another party (such as the Police, Brookes Human Resources or an onsite contractor) seeks access to footage, that party is required to complete the relevant form (Appendix 3) which can be obtained either from contracted Security Services or from the IT Services Information Security Management Team via info.sec@brookes.ac.uk. The third party is required to set out why access is required and how any footage will be used. Members of the IT Services Information Security Management Team will determine whether release is lawful. In the event of a refusal to release footage, the third party can ask the Head of Information Security Management to review that refusal. Footage may be released in the absence of the completion of the form in an emergency. Such release must be authorised by the Head of Information Security Management (or delegated nominee) or a Senior Manager in the Contracted Security Services. The Manager authorising release in this situation is responsible for ensuring that the form be completed retrospectively.

5.6.4 In the interests of processing information only as necessary and in accordance with relevant Data Protection law, the Information Security Management Team may direct the requester to view the footage, rather than receive a copy, if appropriate and practical to do so.

5.6.5 Where CCTV or BWV footage is released within Oxford Brookes and in compliance with the requirements at 5.6.3 above, then it becomes the responsibility of the person who requested it (Appendix 3 section 5) to ensure that any further processing of the released footage is lawful.

5.6.6 The requestor (Appendix 3 section 5) must ensure a lawful ground to process the data has been identified to support any further transfer, viewing or sharing etc. In addition it is the responsibility of the requestor to make sure that only "necessary" personal information is shared. In particular the requestor will make sure that details of individuals who are irrelevant to any investigation or incident are either pixelated or blurred. Footage must be clipped to remove extraneous material. This is to ensure that these individuals cannot be identified from the footage. The ITS Information Security Management Team can advise whether any onward disclosure is lawful as well as the practicalities associated with carrying out this task.

5.7 Retention of Recorded CCTV and BWV Material

5.7.1 CCTV or BWV recordings will be retained on (re-usable if appropriate) media for one calendar month save where a request has been made to retain them by Oxford Brookes University, the Police or a third party who has made a request for the footage to be kept. Then the footage will be kept until it has been copied and supplied to the party requesting it. There may be specific instructions to keep the footage for an indefinite period pending for example a police investigation, where source material is required. The material should be kept until advised otherwise. The contracted Security Services can liaise with the IT Services Information Security Management Team if there is doubt about whether footage should be kept.

5.7.2 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.

5.7.3 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 there has been an incident which was recorded and footage may be required. If there has been such the footage must be be kept for 6 months from the closure of the incident, after which it will be destroyed.

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

Appendix 1 - List of responsible System Managers

1. Deputy Director Commercial and Campus Services
2. Campus Manager – Headington
3. Campus Manager – Harcourt Hill and Wheatley
4. Head of Information Security Management
5. Information Compliance Manager

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

https://www.brookes.ac.uk/estates/meet-the-team/

Appendix 2 – Declaration of Confidentiality

I confirm that my employer [name of employer] has provided me with Information Security Awareness Training relevant to my employment as…….. I am aware of my potential personal liability and implications for my employer from any 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]

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]:*

OXFORD BROOKES UNIVERSITY

Internal CCTV and BWV 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)

Exchanged digitally by encrypted means

5. Declaration and authorisation

I certify that:

- 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 170 of the Data Protection Act, 2018
- I have read and understood the CCTV and BWV Policy and I am aware of all my responsibilities, including those under 5.6.5 - 5.6.6 (about onward processing and the requirement to blur ancillary images of individuals)

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 –Disclosure Request Form (Data Protection Act)

Data Protection Act (2018) Crime and taxation or required to be disclosed by law/ in connection with legal proceedings Request for Disclosure in accordance with Schedule 2 Part 1(2) or Part 1(5)
1. Requestor First name(s): Last name: Job title: Organisation: Address: Postcode: Telephone: Email:
2. Data subject (if known) Current details First name(s): Last name: Address:
Other identifying information (including date of incident and location)

3. Specific information required
4. Reason for requesting disclosure
Offence(s) or suspected offence(s) (please explain why if this information cannot be provided)
6. Purpose **State the purpose for requesting disclosure of personal information about the data subject specified in section 2 of this form. Please specify the statutory powers you rely on here:**
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**
7. Information provision If we hold information how would you like the information to be provided? Electronically using Encrypted Documents or by encrypted transfer* *Encrypted documents will be sent via email and decryption passwords will be 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

8. Declaration and authorisation

The authorising officer must be of the rank of police inspector or higher, or for other 'relevant bodies' a senior officer/manager. An electronic signature is acceptable.

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 could prejudice the case
- The information given on this form is correct and complete to the best of my knowledge

I understand that if any information given on this form is incorrect, I may be committing an offence under Section 170 of the Data Protection Act, 2018

Requestor

Signed:

Date:

Authorising Officer (Requesting Organisation)*
*this must be an officer of the organisation, in a sufficiently senior position to authorise this request: rank of Sergeant or above. An electronic signature is acceptable.

First name:

Last name:

Job title:

Signed:

Date: