



BUCKINGHAMSHIRE  
NEW UNIVERSITY

EST. 1891



# CCTV Protocol



# Contents

Purpose.....	2
Applicability and Scope.....	2
Responsibilities .....	2
Procedures .....	3
The System .....	3
Monitoring and recording of images .....	4
Compliance with Data Protection Legislation .....	5
Access to recorded images .....	6
Applications by third parties. ....	6
Complaints .....	7
Key Relevant Documents.....	7
Appendix One: Equality Impact Assessment .....	8

<b>Approved by:</b>	Health and Safety Committee	<b>Date first published:</b>	Oct-2015
<b>Version:</b>	2.0	<b>Date updated:</b>	Feb-2024
<b>Owner:</b>	Director of Estates and Facilities	<b>Review Date:</b>	Feb-2029

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the University Secretariat.

© Buckinghamshire New University

## Purpose

1. Buckinghamshire New University has in place Closed Circuit Television (CCTV) surveillance systems across the High Wycombe, Uxbridge and Aylesbury campuses, three halls of residence and Missenden Abbey Conference Centre, all operated and controlled by the Estates, Facilities and Services Team.
2. This Protocol details the purpose, use and management of the CCTV systems and outlines the processes to be followed in order to ensure that the University complies with data protection legislation and ICO's guidance on video surveillance for surveillance cameras and personal information.
3. The use of CCTV surveillance must be with respect for the privacy of individuals and the purpose of this Protocol is to ensure that the operation of the CCTV system is consistent with the legal obligations of the University as a Data Controller under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

## Applicability and Scope

4. This code of practice is binding on all University employees and students taught on BNU campuses, all employees of contracted out services and applies to all other persons who may and for whatever reason be present on the University's property.
5. This document must be read in conjunction with other University policies and procedures.
6. The BNU Students Union operates its own CCTV system to cover licencing requirements for the SU Bar and Nightclub and is not part of this Policy.

## Responsibilities

7. **Director of Estates, Facilities and Services**
  - Ensures the overall effectiveness of the Closed-Circuit Television (CCTV) Procedure.
8. **Data Protection Officer**
  - Makes decisions on CCTV disclosures with reference to relevant legislation.
9. **Security Contractor**
  - Operates the CCTV equipment and ensure no unauthorised or inappropriate use is made of the system.
  - Grant and log access to the CCTV footage (including the Control Room), if satisfied as to an individual's identity and that they have a lawful basis and need for access referring to the Data Protection Officer (as necessary).
  - Tests the quality of images to ensure that recorded images and prints as well as live images are clear and fit for purpose and to check that the date and time stamps are correct.

## Procedures

10. The University has installed a CCTV surveillance system for the following purposes:
  - monitoring the premises to enhance safety and security of BNU users and assets;
  - the protection of staff, students, visitors and the assets of the University;
  - the prevention, investigation and detection of criminal or disciplinary offences in accordance with University policies and procedures;
  - the apprehension and prosecution of offenders (including the use of images/data as evidence in criminal/civil proceedings); and
  - to comply with CCTV requirements of Awarding Bodies.
11. BNU seeks to operate its CCTV system in a manner that respects the privacy of individuals while ensuring their safety. The operation of the CCTV system has been established to ensure it is consistent with the legal obligations of the University including in its role as a Data Controller. The CCTV system will be used to observe the University's campuses and areas under surveillance in order to identify incidents requiring a response. Any response will be proportionate to the incident.
12. The external cameras generally cover the perimeter of the University buildings, car park areas and approaches to the Campus. Internal cameras generally cover transit spaces such as corridors, social/communal and reception areas. CCTV is required in areas that are used for testing requirements stipulated by Awarding Bodies.
13. All CCTV cameras in general use are configured to record images only; any sound recording facilities are switched off or disabled. CCTV cameras used during examinations may include the facility to record sound in accordance with the assessment body requirements.
14. Cameras are a combination of fixed and Pan/Tilt/Zoom (PTZ). Cameras are not sited to focus on private residential areas or other areas of private property or office spaces.
15. All cameras are currently deployed on either fixed or pre-set trajectories. In real-time, where a security incident has been identified by the CCTV operator, for example an individual is suspected of suspicious or anti-social behaviour such as a bike theft or illegal parking, PTZ cameras can be used to observe the situation and the individual(s) involved. At no time will a camera be directed to follow or track an individual unless it is believed a criminal offence is being committed.
16. The CCTV system is operational and is capable of being monitored for 24 hours a day, every day of the year.
17. Any proposed new CCTV installation is subject to a Data Protection Impact Assessment.

## The System

18. The CCTV systems are owned and managed by Buckinghamshire New University, Queen Alexandra Road, High Wycombe, HP11 2JZ with a maintenance contract in place a third-party provider(s). The University is the Data Controller for the images produced by the CCTV system

and is registered with the Information Commissioner's Office, registration number Z772474X. The operation of the CCTV system meets the requirements of data protection law and the Information Commissioner's CCTV Code of Practice.

19. BNU users and the public are made aware of the presence of CCTV by clear signs notifying that CCTV is in operation, identifying the University as the Data Controller, providing contact details for the University and, as far as possible, setting out the purposes and legal basis for processing the CCTV images. The processing of CCTV data is also outlined in the CCTV Privacy Notice available on the BNU website.
20. CCTV equipment will be maintained and tested in accordance with a regular schedule. This will be managed under the maintenance contract BNU has with a third-party provider(s). The Security Contractor will be responsible for testing the quality of images to ensure that recorded images and prints as well as live images are clear and fit for purpose and to check that the date and time stamps are correct.

## **Monitoring and recording of images**

21. The CCTV system shall be operated and maintained in accordance with this Protocol, which is available on the University web pages or in hard copy by request. All Campus Officers involved in the operating and monitoring of CCTV should familiarise themselves with the Protocol and make sure they are aware of their responsibilities. Data Protection training will be provided to Campus Officers and their Managers and documented by the Data Protection Officer.
22. Cameras are monitored in the campus security control room at each location, which is a secure room and only accessed by campus security officers and their Managers for this purpose. CCTV can be monitored 24 hours a day at the allocated campus security offices and remotely in the 24hr High Wycombe security control room. Each time equipment is accessed a user identification and password must be entered by authorised personnel. All actions on the equipment are logged against the login ID. This helps ensure that there is an auditable trail.
23. CCTV cameras must not be trained on private residences or properties/areas where it is not clear that CCTV is operating and it would not be expected. If cameras do capture images of such areas, electronic privacy masks should be in place or reasonable adjustments made to prevent this.
24. Images are recorded locally at each Campus on disk recorders that are overwritten every 30 days. Where an incident occurs or a Subject Access Request is made, the CCTV images may be saved to servers located securely on the University infrastructure. These should be deleted once no longer needed.
25. It is expressly forbidden to make or take any recordings of or from the CCTV digital recording systems without proper cause.
26. Body worn cameras may be used in key areas, such as during Security patrol duties at halls of residences. The downloading of images from such cameras will only be conducted by trained security staff and cameras will be cleansed following each shift.

27. Security staff wearing body worn cameras will disclose, when approaching persons, that they are being video and audio recorded.

## **Compliance with Data Protection Legislation**

28. In its administration of its CCTV system, BNU complies with relevant data protection law. In particular, due regard is given to the data protection principles contained in the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. The principles provide that personal data must be:
- a) processed lawfully, fairly and in a transparent manner;
  - b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
  - c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  - d) accurate and, where necessary, kept up-to-date;
  - e) kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
  - f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
29. Signs are placed at all pedestrian and vehicular entrances in order to inform staff, students, visitors and members of the public that CCTV is in operation. The signage indicates that the system is managed by BNU and a 24 hour contact number is provided.
30. The systems in use are digital. Recorded images will be retained for no longer than required for the purpose for which they were originally obtained, and images are automatically overwritten (currently 30 days).
31. Should images need to be retained for any reason, including for release to a third party such as the Police or a data subject, copies of those images may be transferred to an appropriate computer file. In this instance, and if BNU needs to keep footage or images longer than the 30-day default period, for example as evidence in the detection of a crime or ongoing investigation, then copies of the relevant images will be transferred to a securely encrypted computer file. A record/audit trail must be kept of the handling of any images (e.g. using a Subject Access Request Log) to ensure that rights of individuals are preserved and that the chain of evidence remains intact should the images be required for evidential purposes. Once there is no longer a legitimate reason to retain the images, they must be deleted/disposed of securely.
32. CCTV recordings for the purpose of Awarding Bodies, will be held in accordance with the Records Retention Schedule.

## Access to recorded images

33. A data subject or anyone who considers that they may be a data subject in terms of the University potentially holding their personal information, has the right to request details of any personal data held by BNU relating to them. This includes a right to request copies of images recorded by the University's CCTV system. Such a request is called a Subject Access Request (SAR) and is listed as one of the rights of the data subject under Article 15 of the GDPR ('the right of access'). Note that SAR's must be answered within one month of receipt and recorded in the SAR's log by the Data Protection Team.
34. Requests by individual data subjects for CCTV images relating to themselves should be directed to:  
Data Protection Officer  
Buckinghamshire New University  
Queen Alexandra Road  
High Wycombe HP11 2JZ  
Email: [dpofficer@bnu.ac.uk](mailto:dpofficer@bnu.ac.uk)
35. In order to locate the images on the CCTV system, sufficient detail must be provided by the data subject so that the relevant images can be located, and the data subject can be identified.
36. BNU has a procedure in place to handle data subject requests and a 'Data Subject Request Form' for anyone who wants to make a subject access request. It is requested that people use this form, if possible, as it helps to identify the personal information they would like to access and provide a quick response. However, if a request is made by email or some other written format it should be processed without using the form. A request can also be made verbally.
37. The University will acknowledge all requests upon receipt and will provide a full response within one month from the date of receipt, as required under data protection law, unless an exemption applies. To safeguard the information it holds and to ensure the privacy of individuals, BNU is entitled to ask for such evidence as it may reasonably require, so it may verify the identity of the individual making the request before any information is provided.
38. Where the University is unable to comply with a Subject Access Request without disclosing the personal data of any other individual who is identified or identifiable from that information (i.e. someone else appears in the image with the data subject), it is not obliged to comply with the request unless the other individual has consented to the release of the images or can be removed from the images.

## Applications by third parties.

39. Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system, for example when disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances specified in the relevant legislation.
40. Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or Director of HR, CCTV images may be provided for use in staff or student disciplinary cases.

41. All activity on the CCTV system is automatically logged against users. Details of all access to the CCTV equipment by non-authorised personnel will be recorded in a log accessible in the Campus Office that will include name of member of staff handling request, name and contact details of individual who the recording was handed to, who authorised access, relevant paperwork and reason for access.
42. The Security Contractor at each campus is responsible for the operation of the CCTV equipment and for ensuring no unauthorised or inappropriate use is made of the system. Only personnel who have received full training on the operation and use of the CCTV equipment shall be authorised to operate the equipment.
43. In an emergency, and where it is not reasonably practicable to secure prior authorisation, the Security Contractor may grant access to the Control Room, if satisfied as to the individual's identity and that they have a legitimate reason and need for access.
44. With the exception of law enforcement bodies in the instance of crime and Subject Access Requests (where an individual, or someone they have agreed to act on their behalf, for example a solicitor asks to access their data, see paragraph 30 above) images will not be provided to third parties. Such disclosures will be made at the discretion of the Data Protection Officer with reference to relevant legislation.

## **Complaints**

45. Complaints concerning the University's use of its CCTV system or the disclosure of CCTV images should be made in writing to the Director of Estates and Facilities or the Deputy Vice-Chancellor.
46. Any use of the CCTV system or materials produced which is outside this protocol and is inconsistent with the objectives of the system will be considered gross misconduct.
47. Misuse of the system will not be tolerated; continuing public support is vital. Any person found operating outside these codes without good and reasonable cause will be dealt with under the University disciplinary system. If any breach constitutes an offence under criminal or civil law then court proceedings may be taken.
48. Any complaint concerning misuse of the system will be treated seriously and investigated by the Director of Estates or deputy and the Deputy Vice-Chancellor.
49. Where appropriate the Police will be asked to investigate any matter recorded by the CCTV system which is deemed to be of a criminal nature.

## **Key Relevant Documents**

- Data Protection Policy
- Freedom of Information Policy
- Information Security and Data Breach Management Procedures
- Data Subject Access Request Procedures

## Appendix One: Equality Impact Assessment

<b>1. What is changing and why?</b>				
This protocol is being reviewed according to the review schedule.				
<b>2. What do you know?</b>				
This protocol is a factual and procedural document, providing clear guidelines around the use of CCTV, the purpose of having CCTV, the type of data recorded and the length of time data is held. Equalities and the rights of individuals are at the fore.				
<b>3. Assessing the impact</b>				
	<b>Could benefit</b>	<b>May adversely impact</b>	<b>What does this mean?</b> <i>Impacts identified from what you know (actual and potential)</i>	<b>What can you do?</b> <i>Actions (or why no action is possible) to advance equality of opportunity, eliminate discrimination, and foster good relations</i>
a) How could this affect different ethnicities? <i>Including Gypsy, Roma, Traveller, Showmen and Boaters, migrants, refugees and asylum seekers.</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	This protocol does not distinguish between or affect differently people of different ethnicities however it is acknowledged that certain groups may feel targeted / watched more due to their ethnicity due in part to the current climate of anti-terrorism measures.	The use of CCTV is governed by legislation and national codes of practice. The Director of Estates or nominated deputy is responsible for providing guidance to officers on the use of CCTV system. Existing policies procedures and guidance will provide wider public reassurance around the robustness of systems and governance.
b) How could this affect cisgender and transgender men and women (including maternity/pregnancy impact), as well as non-binary people?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This protocol could have a positive impact as those individuals with this characteristic may feel safer in areas covered by CCTV.	
c) How could this affect disabled people or carers? <i>Including neurodiversity, invisible disabilities and mental health conditions.</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	This protocol does not distinguish between or affect differently people with a disability however it is acknowledged that those with a visual impairment may not be able to see signs informing people on the use of CCTV	The policy is available on the BNU website therefore is available in different fonts, text size and through assistive technology.
d) How could this affect people from different faith groups?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	It is not envisioned that there will be any direct impact on people from different faith groups as the protocol applies to everyone. Therefore, there should be no difference in how individuals who share this protected characteristic are treated.	
e) How could this affect people with different sexual orientations?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This protocol could have a positive impact on those people with different sexual orientation who may be the subject of hate incidents.	

			CCTV coverage may make then feel reassured.	
f) How could this affect different age groups or generations?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This protocol does not distinguish between or affect differently people from different age groups or generations. It protects the interest of all users.	
g) How could this affect those who are married or in a civil partnership?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	It is not envisioned that there will be any direct impact on people who are married or in a civil partnership as the protocol applies to everyone. Therefore, there should be no difference in how individuals who share this protected characteristic are treated by the policy.	
h) How could this affect people from different backgrounds such as: socio-economic disadvantage, homeless, alcohol and/or substance misuse, people experiencing domestic and/or sexual violence, ex-armed forces, looked after children and care leavers.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This protocol does not distinguish between or affect differently people from different backgrounds. However it is acknowledged that individuals in this group may feel targeted / watched more due to their background. Conversely, some individuals may feel safer knowing that CCTV is in use.	
i) How could this affect people with multiple intersectional experiences?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	CCTV has the ability to have a positive impact across all the equality groups as its main purpose is to prevent and reduce crime; and reduce the fear of crime for anyone studying, working or visiting BNU.	
<b>4. Overall outcome</b>				
No major change needed <input checked="" type="checkbox"/>	Adjust approach <input type="checkbox"/>	Adverse impact but continue <input type="checkbox"/>	Stop and remove <input type="checkbox"/>	
<b>5. Details of further actions needed</b>				
n/a				
<b>6. Arrangements for delivery and future monitoring</b>				
The policy will be reviewed in accordance with the review schedule.				
<b>7. Completed by:</b>	Jenny Horwood	Information Governance Manager (Interim)	<b>Date</b>	12-March-2024
<b>8. Signed off by:</b>	Paul Robinson	Director of Estates and Facilities	<b>Date</b>	14-March-2024



**High Wycombe Campus**  
Queen Alexandra Road  
High Wycombe  
Buckinghamshire  
HP11 2JZ

**Aylesbury Campus**  
59 Walton Street  
Aylesbury  
Buckinghamshire  
HP21 7QG

**Uxbridge Campus**  
106 Oxford Road  
Uxbridge  
Middlesex  
UB8 1NA

**BNU based at  
Pinewood Studios**

Pinewood Studios  
Pinewood Road  
Iver Heath  
Buckinghamshire  
SL0 0NH

**Missenden Abbey**  
London Road  
Great Missenden  
Buckinghamshire  
HP16 0BD

**Telephone: 01494 522 141**

 [BucksNewUni](#)

 [BucksNewUni](#)

 [BucksNewUni](#)

 [BucksNewUniversity](#)