PRIFYSGOL
BANGOR
UNIVERSITY

Code of Practice on Closed Circuit Television (CCTV)

Date	Purpose of Issue/Description of Change	Equality Impact Assessment Completed
December 2011	Initial Issue	
5th June, 2017	Review and approval by Compliance Task Group	4th July, 2017
28th January 2019	Review and re-approval by Compliance Task Group	
22nd September 2022	Review and re-approval by Compliance Task Group	
2nd August 2023	Amendments to update roles and responsibilities	

Policy Officer	Senior Responsible Officer	Approved By	Date
Head of Legal Services	Director of Estates and Campus Services	Compliance Task Group	22nd September 2022

This Code of Practice will be reviewed in 3 years

1. Introduction

The monitoring, recording, holding and processing of images of identifiable individuals constitutes personal data as defined by the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA18). This Code of Practice is intended to ensure that in its use of CCTV Bangor University is fully compliant with the requirements of the GDPR and DPA18, and with related legislation. It should be read in conjunction with the University's Data Protection Policy.

The Code of Practice has also been informed by the Information Commissioner's Office guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv/
and the Amended Surveillance Camera Code of Practice: https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version

2. Scope of the Code

This Code of Practice is binding on all staff and students of Bangor University and all other persons who may, for whatever reason, be present on University property at any time.

This Code of Practice covers not only the main CCTV infrastructure within the University, the viewing facilities in particular University buildings (e.g. Pontio, Canolfan Brailsford) but also any standalone CCTV systems within individual schools and departments, including any connected technology and devices (e.g. Braint Shop etc.).

3. Ownership and Operation of the CCTV System

Bangor University owns all CCTV systems on its campus, operated in accordance with the purpose outlined in Section 4. below. The main CCTV system is operated by the University's Campus Services and day-to-day management of the system is the responsibility of the Security and Response Manager. Only authorised staff will operate any of the equipment located within the CCTV control room. The CCTV system(s), all recorded material and copyright is owned by Bangor University.

No member of University staff, student, visitor, volunteer or contractor can set up a CCTV system (including web cameras or time lapse capture devices) on Bangor University premises without authorisation from the Director of Estates and Campus Services.

4. Purpose

CCTV systems are utilised at Bangor University for the following specific purposes:

- To discourage delinquent and anti-social behaviour;
- To deter and detect crime, including theft and criminal damage;
- To enhance the safety and well-being of staff, students and members of the public;
- To assist in the overall management of all University owned buildings.

Where, in the carrying out of these purposes, images are obtained of persons committing acts of an illegal / criminal nature and / or acts which breach the University's Rules and Regulations these images may be used as evidence, either internally or in accordance with law enforcement agencies.

Bangor University CCTV systems must not be used for purposes other than those specifically indicated above.

5. Approval and Registration

Any new requests for the installation of CCTV on Bangor University premises must be made using the appropriate form (see Appendix 3) and should be sent to the Security and Response Manager within Campus Services. In consultation with the Data Protection Officer or the Head of Legal Services an initial Data Privacy Impact Assessment will be carried out taking into account what benefits can be gained from the new system, whether better solutions exist, and what effect it may have on individuals.

If it is considered that CCTV is appropriate the request will be forwarded to Campus Services to assist the College / School or Department with an analysis of needs and costs.

Each part of the proposed new system must fully comply with the provisions of this Code of Practice. A central register will be maintained, held by the Security and Response Manager, listing the location of all cameras and associated equipment.

6. Location and Sites

The following guidelines must be observed when installing CCTV systems on Bangor University premises:-

- Apart from in exceptional circumstances (see 7 below) cameras must not be hidden from view and must be sited in such a way as to ensure that they only monitor the areas intended to be covered;
- Signs must be prominently displayed so that everyone is aware that they are entering a zone that is covered by surveillance equipment;
- Signs must indicate the purposes for which cameras are installed and the contact details for the manager of the scheme.
- A Data Privacy Impact Assessment will be undertaken prior to approval of any new or relocated cameras

The University's approved wording for CCTV signage can be found in Appendix 2 below.

In accordance with University policies and procedures, all work to the estate, including any work associated with CCTV systems, must be managed via Campus Services. This includes any surveys and / or inspections which require access to voids, ceiling spaces and other parts of the estate not normally accessed.

7. Covert Monitoring

Covert use of Bangor University CCTV systems can only take place on the written permission of the Chief Operating Officer or their nominee. For monitoring to occur there must be reasonable cause to suspect that unauthorized or illegal activity is taking place, or is about to take place, or that a breach of the University's Rules and Regulations is taking place, or is about to take place. Covert monitoring will only be undertaken for a limited and reasonable period of time consistent with the documented objectives. All decisions relating to the use of covert monitoring will be fully recorded.

Where a legitimate third party (e.g. a law enforcement agency) wishes to undertake covert monitoring using University premises the request should be brought to the Data Protection Officer and/or Head of Legal Service's attention in the first instance, who will discuss it with, and obtain approval from, the Chief Operating Officer or their nominee.

8. Access to and disclosure of CCTV images

[a] Principles

It is important to ensure that access to and disclosure of CCTV images is restricted and carefully controlled not only to safeguard the rights of individuals but also to ensure that any evidence remains intact should the images be required in the future for evidential purposes.

Local CCTV operators (including those with viewing facilities) must:

- Restrict access to those staff who need to have access to the recorded images for the purpose(s) for which the system was installed;
- Make practical arrangements for ensuring that recorded images are only viewed by authorised staff in a secure and confidential location;
- Ensure that the CCTV log records all access to and disclosure of CCTV images.

[b] Access to CCTV images

Arrangements for access to Bangor University CCTV images are covered by the University's Data Protection Policy. All Bangor University CCTV operators must ensure that:

- All requests from individuals for access to their images are dealt with under the Data Subject Access procedure by the Data Protection Officer in consultation with the Security and Response who will arrange access once appropriate identification checks have been carried out;
- Images are not disclosed to any third parties (including staff who are not authorised to view them);
- Images disclosed will, where necessary, include appropriate measures to protect the identity of other individuals. The Security and Response Manager will oversee, and sign off, this process prior to disclosure;
- All requests from the police for access or disclosure should be directed to the Safeguarding, Conduct and Complaints Coordinator within Governance Services in the first instance (or in their absence the Data Protection Officer) and the procedure outlined in the *Disclosure Procedure: Request for Information by Law Enforcement Agencies* should be followed.
- All requests from University Colleges, Schools or Central Services for access to images will be dealt with by the Safeguarding, Conduct and Complaints Coordinator in the first instance in consultation with the Security and Response Officer
- The University will retain CCTV images for 14 days unless an incident is recorded which requires further investigation either by the University, by the Security Services, the police or another external body with prosecuting powers.

Access to the main University CCTV system must only be given as outlined in Section [c] below, no unauthorised access should be given to areas of the University where viewing facilities are located (e.g. Pontio, Canolfan Brailsford etc.). Access to these local viewing facilities are strictly restricted to on duty key staff only (appropriate staff to be agreed in consultation with the Security and Response Manager, the Director of Campus Services

[c] Access to the CCTV Control Rooms

Access to the CCTV monitoring and recording equipment is strictly restricted to on duty security staff only for lawful, proper and sufficient reasons. All other members of staff and/ or visitors are prohibited from entering the CCTV Control Rooms without prior approval from the Security Team Leader or another member of the on duty Security staff.

Visits will not take place as a matter of routine. Staff and / or visitors will always be accompanied by a Team Leader or another member of the on duty Security staff. All visitors to the CCTV Control Room must read and sign the confidentiality agreement attached as Appendix 1 of this Code and sign the Control Room log book.

This process will be reviewed on a monthly basis by the Operations Manager (Security).

9. Emergencies and Major Incidents

In the event of an emergency or a major incident the police will be given authority to view images in the CCTV control room. Such authority will be given by the on duty Security Team Leader, Security and Response Manager, Head of Facilities or Director of Estates and Campus Services verbally, and noted in the daily log.

No images are to be handed over to the police without following the procedure in 8[b] above. If, however, images are required immediately to deal with an ongoing police incident the Security Team Leader or another member of the on duty Security staff should follow the process outlined in the *Disclosure Procedure: Request for Information by Law Enforcement Agencies.*

10. Monitoring and Review

This Code of Practice on CCTV will be kept under review by the Compliance Task Group and a yearly audit will be carried out by the Security and Response Manager to monitor the requirements of this Code of Practice. Any questions about its interpretation or operation should be referred to the Director of Estates and Campus Services in the first instance.

11. Misuse of the System and Complaints

Any use of Bangor University CCTV system which is outside this Code and is inconsistent with the purposes stated in 4 above will treated seriously by the University and may be considered under disciplinary procedures.

The Data Protection Officer will coordinate any complaints received in respect of this policy in consultation with the Security and Response Manager.

- The complaint should be addressed to the Data Protection Officer in the first instance. The complaint will be acknowledged immediately and every reasonable effort will be made to offer a more comprehensive reply within 21 days.
- If the applicant is not satisfied with the reply then they should inform the Chief Operating Officer within 21 days, and will be dealt with in accordance with the University's Staff & General Complaints Procedure or the University's Student Complaints Procedure as appropriate.

APPENDIX 1

CCTV: Confidentiality Document

To be read by all visitors to:-

[a] a Bangor University CCTV Control Room; or

[b] any Bangor University CCTV viewing or recording facility; or

[c] any area of the University where CCTV images are processed.

Entry to this controlled CCTV area is accepted on the condition that the visitor agrees to abide by the requirements of the Bangor University CCTV Code of Practice, the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.

In brief, these are outlined as follows:-

All images viewed by persons visiting the control room must be treated as confidential.

No unauthorised disclosure shall be made by any persons of the contents or subject matter of images, which is defined as data under the Data Protection Act 2018.

Any breach of disclosure rules may make the person disclosing personally liable to prosecution under the Data Protection Act 2018. Any such disclosure will not be with the permission or authority of the Data Controller or other partners in the CCTV scheme.

APPENDIX 2

Approved bilingual wording for all Bangor University CCTV signage:-

> Mae delweddau'n cael eu gwylio a'u cadw at bwrpas atal troseddu a diogelu'r cyhoedd. Rheolir y cynllun hwn gan Brifysgol Bangor. Am fwy o wybodaeth ffoniwch 01248 382795.
>
> Images are being monitored and recorded for the purposes of crime prevention and public safety. This scheme is controlled by Bangor University. For more information, call 01248 382795

It is University procedure that signs should be placed at the entrance to all CCTV areas. It is particularly important that signs are clear and prominent where the cameras themselves are very discreet, or in locations where people might not expect to be under surveillance. Advice should be sought from the Security and Response Manager on appropriate locations for signs.

APPENDIX 3

APPLICATION FORM FOR NEW CCTV SYSTEM /
AMENDMENT TO EXISTING CCTV SYSTEM

Please be aware that all new CCTV systems at Bangor University are to be Digital IP cameras

A. CONTACT DETAILS

Contact name: _____

College / School / Department: _____

Tel: _____ Email: _____

B. SUPPORTING EVIDENCE

[i] Rationale

Please address issues such as:

- *What are the benefits to be gained from its use,*
- *Can CCTV technology realistically deliver these benefits,*
- *What effect would the CCTV system have on individuals*
- *Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives*
- *Do you need images of identifiable individuals, or could the system use other images not capable of identifying the individual?*

_____

_____

_____

_____

_____

[ii] Location of system:

_____

[iii] Purpose of system (*Please tick one purpose)*

Recognition ☐

(Sufficient for recognition but not sufficient for identification of an offender without further evidence)

Identification ☐

(Can be used for identification and admissible in Court)

C. SPECIFICATIONS AND COSTINGS

Specifications and costings will be drawn up in consultation with Property and Campus Services. Before submitting this form a College / School or Department should be in a position to finance the scheme – if a ball-park figure is required for further consideration please contact the Campus Services Manager (Security))

[i] Required Specification

No of fixed cameras: _____ Specification: _____

No of Tilt & Pan cameras: _____ Specification: _____

No of other cameras: _____ Specification: _____

Diagram / location plan showing proposed location of camera(s) included ☐

[ii] Cost Code

Cost Code for payment of scheme: _____

Please note: Authorization should be sought for any proposed system and / or upgrade prior to purchase and / or installation.

D. DECLARATION

I confirm that this request is in line with the College /School / Department's requirements and that the appropriate funds have been identified.

Name: _____ Signed: _____
(Head of College / School / Department)

Date: _____

Once signed by the Dean of College / Head of School / Director of Professional Service this form should be sent to the Security and Response Manager, via the Campus Services Helpdesk who will undertake a Privacy Impact Assessment in consultation with the Data Protection Officer.

Campus Services Helpdesk: campusservices@bangor.ac.uk

Review and Data Privacy Impact Assessment Complete (and attached)

Signed: _____ Date: _____

(Campus Services Manager (Security))