Ollscoil na Gaillimhe
University of Galway

Polasaí agus Nósanna Imeachta/Policies and Procedures

Code	QA170
Title	Closed Circuit Television (CCTV) Systems
Policy Owner	Director of Buildings and Estates
Date	24 02 2026
Approved By	University Management Team

1. Policy Statement

1.1. University of Galway has a statutory responsibility to protect the security and safety of all students, staff, visitors, and contractors and any campus user whilst on University of Galway premises.

1.2. All personal data processing will be done in accordance with relevant legislation and in accordance with the University of Galway Data Protection Policy (QA400). University of Galway is the Data Controller of the personal data collected unless otherwise identified. The personal data collected will include images and movements of University of Galway students, staff, visitors, contractors and private individuals.

1.3. This Policy is informed by the principles set out in the General Data Protection Regulation (GDPR), National Data Protection Law and the Freedom of Information Act 2014, together with guidance issued by the Office of the Data Protection Commissioner and/or the Office of the Information Commissioner and from the Code of Practice for CCTV Systems authorised under section 38(3)(c), of the Garda Síochána Act 2005.

1.4. All references to video surveillance systems consisting of Closed Circuit Television (CCTV) are hereinafter referenced as CCTV.

1.5. The use of CCTV systems is an integral and deemed justified part of enhancing the safety and security of the University of Galway campus. The operational system for security at University of Galway uses CCTV to compliment alternative security measures in place at the University.

1.6. Due to the nature of the sites day-to-day operations, it is necessary to operate CCTV 24 hours a day.

1.7. The use of the CCTV system is conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy.

2. Scope of the policy

2.1. This policy applies to the use of CCTV systems (CCTV, ANPR, BWC or cameras) across all areas of the University of Galway premises, both internal and external on the main University of Galway city campus and on all outlying campus areas.

2.2. This policy applies to all employees, students, agents, visitors and all other campus users.

2.3. This policy does not cover any CCTV system where University of Galway is not a Data Controller and where University of Galway is not the sole operator of said CCTV system.

3. Purposes of the policy

3.1. The purpose of this policy is to regulate and outline the safeguards in place in the University of Galway regarding the operation, monitoring and access to CCTV systems and images, and it will be used for the purposes included but not limited to:

3.1.1. To protect University of Galway staff, students, visitors and University of Galway premises, both during and after core hours.

3.1.2. To protect, deter and prevent crime, violence, vandalism, anti-social behaviour, and to detect and investigate health and safety, security, campus/building/room access/egress, legal claims and legal affairs relating to University of Galway.

3.1.3. To assist general site management, including human and vehicular traffic management, fire prevention and management, at the University of Galway premises.

3.1.4. To assist University of Galway in fulfilling its data protection, freedom of information and other statutory obligations including requests for access. University of Galway reserves the right to refuse a request, if such request was unreasonable or proves to be cost prohibitive.

3.1.5. To assist University of Galway in mandatory reporting to An Garda Síochána and/or other Competent Authority, University insurers and their designates, in investigating allegations of crimes, accidents and incidents, as required.

3.1.6. To protect health and safety, security, crime prevention and legal affairs and legal claims at University of Galway student accommodation.

3.1.7. To assist University of Galway to monitor occupancy and usage of University buildings.

3.2. Data obtained using CCTV systems shall be limited and proportionate to the purposes for which it was obtained.

3.3. The CCTV systems will not be used by University of Galway for any other purposes other than those outlined in this policy.

4. Responsibilities

4.1. Security Services Supervisor

4.1.1. Ensure that the use of CCTV systems and the monitoring of all footage are carried out in accordance with this policy.

4.1.2. Ensure that all monitoring is carried out in compliance with any relevant legislation relating to privacy.

4.1.3. Ensure that only authorised individuals have access to footage and only as necessary.

4.1.4. Oversee the use of CCTV monitoring for safety and security purposes across University of Galway premises.

4.1.5. Co-ordinate viewing and release of any footage with the parties involved, i.e. An Garda Síochána.

4.1.6. Arrange and oversea release of redacted footage, on foot of a valid reasonable request. Maintain a record of the release of any footage.

4.1.7. Ensure that any required signage is correct and in place, including information on how to contact the individuals responsible for the system and footage and details of the Data Controller**.**

4.1.8. In the event of an incident being reported to the University of Galway Security Office, the footage of the identified location will be reviewed by the Security Office. University of Galway's DPO and /or Legal Counsel's advice will be sought, as necessary.

4.2. References in this policy to any roles or responsibility of the Security Services Supervisor may be delegated in their absence or unavailability to the Head of Facilities Management and Services, the Facilities Manager or to a specific designated member of the Security Team.

4.3. Security companies that place and operate cameras on behalf of University of Galway are "Data Processors." As data processors, they operate under the instruction of the University of Galway. Article 32 of the GDPR places several obligations on data processors. These include having appropriate security measures in place to prevent the destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, in particular where the processing involves the transmission of data over a network and against all unlawful forms of processing. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted. Staff of the security company have been made aware of their obligations relating to the security of data.

5. Recording and retention

5.1. CCTV/BWC/ANPR installed at University of Galway premises uses digital recording technologies only.
5.2. Recordings are made directly to storage device.
5.3. Recordings by CCTV/ANPR are retained for a period not exceeding one month, unless specifically required for investigation/ security/safety/legal purposes, in accordance with Data Retention Schedule and Guidance (QA442).
5.4. Each set of copied recorded material for CCTV/ANPR extracted from the system has assigned to it a unique tracking reference and will be transferred in a secure encrypted method to the relevant recipient. This may be through physical or digital means. The Security Services Supervisor, in consultation with the Data Protection Officer, as required, to review and access the necessity and proportionality of continued retention of CCTV/BWC/ANPR retained for evidence. In the event of an ongoing law enforcement investigation the data will be retained until such time as the footage is no longer required for the investigation. In the case of incident notified to University insurers, the data will be kept until such time as the as the case is closed, or where no claim is made the data will be retained for the period of the statute of limitations plus 13 months.

6. Legal basis for processing of personal data

6.1. University of Galway relies upon the following legal basis for processing personal data:
6.1.1. Processing is necessary for compliance with a legal obligation (Article 6.1(c) of the GDPR); examples include but not limited to duty of care as ascribed to an employer under Health and Safety at Work Act 2005, and common duty of care ascribed to an occupier of a premises under the Occupiers Liability Act 1995.
6.1.2. Processing is necessary for the purposes of the legitimate interests of the University of Galway (Article 6.1(f) of the GDPR), based on the purposes set out in this policy.
6.1.3. For all processing of personal data not covered under the University's legal obligations or legitimate interests, the University relies upon the legal basis of public task in the public interest and in its exercise of official authority, to perform the object and functions of the Universities Act, 1997 (Article 6.1(e) of the GDPR, section 12 and 13 of the Universities Act, 1997).
6.2. University of Galway relies upon the following legal basis for processing of special categories of personal data:
6.2.1. Processing is necessary to protect the vital interests of University staff, students, visitors and members of the public or any person(s), including those may be trespassing, or who ordinarily should not be on the University of Galway premises (Article 9.2(c) of the GDPR).
6.2.2. Processing is necessary for establishing, exercise or defending legal claims (Article 9.2(f) of the GDPR).

7. Disclosure of personal data

7.1. Access to CCTV/BWC/ANPR footage will be strictly confined to the nominated University of Galway staff and contractors. In certain circumstances, the footage may be released, in line with this policy and pursuant to relevant legislation.
7.2. Law Enforcement bodies may request CCTV/BWC/ANPR footage under Section 41 of the Data Protection Act, 2018. Such requests must be reviewed by the Data Protection Office and/or Security Services Supervisor and must comply with the following requirements:
7.2.1. The request must be set out in writing.
7.2.2. The request must indicate the request is made under section 41 of the Data Protection Act, 2018.
7.2.3. The request must be signed and dated by a Garda member not below rank of Sergeant and must include an identification number.

7.2.4. The request must set out the details of the CCTV recording required.

7.3. Data protection legislation provides individuals with a right to access their personal data. CCTV footage of an individual constitutes their personal data, as defined by Article 4(1) of the GDPR. An individual can submit a Data Subject Access Request to the Data Protection Office, in writing, at dataprotection@universityofgalway.ie. Data Subject Access Request procedure is detailed in Data Subject Rights Request Procedure (QA444).

8. Implementation and review

8.1. The policy will be reviewed as required in light of any legislative or other relevant developments, taking cognisance of changing information or guidelines from the Data Protection Commissioner, An Garda Síochána, and the internal policies of University of Galway.

9. Complaints procedure

9.1. Individuals have the right to object to processing of their personal data and may do so by contacting the Data Protection Office at dataprotection@university.ie.

9.2. Anyone not satisfied with the manner University of Galway handles their personal data, is entitled to make a complaint to the Data Protection Commissioner who may investigate the matter for them. The Data Protection Commissioner's website is www.dataprotection.ie or can contacted at their Office at:

Data Protection Commission
6 Pembroke Row
Dublin 2
D02 X963
Ireland

10. Related documentation

10.1. Appendix 1 – Definitions
10.2. Appendix 2 – Body Worn Cameras
10.3. Appendix 3 – Number Plate Recognition

11. Responsibilities

Name	Responsibility
Director of Buildings and Estates	Policy Owner
Security Services Supervisor	Revisions and updates to policy. Maintaining copies of the policy on University website.
All Staff	Acquaint themselves with, and abide by, the rules set out in this Policy in relation to CCTV; Report any breaches of the policy in a timely manner.

Appendix 1
Definitions

Automatic Number Plate Recognition (ANPR) means systems that have the ability to collect and analyse large quantities of personal data in real time data when vehicles drive past their field of vision. In particular the number plate of vehicles.

Body Worn Camera (BMW) means the use of cameras that are worn by a person and are often attached onto the front of clothing or a uniform or headgear. These devices are capable of recording both visual and audio information.

Cloud Computing means the delivery of computing service, servers, storage, databases, networking, software, analytics, intelligence and more over the Internet ("the cloud") to offer faster innovation, flexible resources and economies of scale.

Closed-Circuit Television (CCTV) means the use of video cameras to transmit a signal to a specific, limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted. It includes live or recorded footage consisting of pictorial, optical or audio-visual means, including but not limited to image, image/photographical stills, picture frame, video, audio, any combination thereof and/or the combination of extracts or snippets thereof relating to systematic monitoring of live or recorded publicly accessible areas at University of Galway sites. Furthermore, it relates to images that are partially obscured, pseudonymised or redacted where a link back to re-identify individuals contained in the CCTV exists at University of Galway.

Cyber Security Incident means any malicious act or suspicious event that compromises or is an attempt to compromise IT systems and networks or the security controls used to protect the IT systems and networks.

Data means all footage and or any portion of same where archived from CCTV footage, including but not limited to image, video, audio and metadata.

Data Protection Legislation means all applicable laws and regulations relating to the Processing of Personal Data and privacy including the Data Protection Act 2018, the General Data Protection Regulation 2016/679 (the "GDPR") and the European Communities (Electronic Communications, Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. 336/2011) and any statutory instrument, order, rule or regulation made thereunder, as from time to time amended, extended, re-enacted or consolidated.

Data Controller means University of Galway for the purpose of this policy.

Data Subject Rights means the rights of the data subject set out in the GDPR (2016/679) with particular regard to articles 12 to 23.

Data Protection Impact Assessment (DPIA) means a process designed to identify risks arising out of the processing of personal data prior to the processing of personal data, with the aim of minimising these risks as far and as early as possible. DPIAs are important tools for negating risk and for demonstrating compliance with the GDPR.

Encryption/Encrypt means the process of converting (encoding) information from a readable form that can be read by everyone into an unreadable form (cipher text) that can only be read by the information owner and other authorised persons possessing the decryption key.

Erasure a means the total and irreversible deletion of footage data, including the blurring and/or irreversible redaction of camera footage including any related extracts, stills or snippets, back up camera footage or copies thereof.

General Data Protection Regulation (GDPR) means Regulation 2016/679.

Personal Data, Processing (and like words), Restriction of Processing, Profiling, Pseudonymisation, Filing System, Controller, Processor, Recipient, Third Party, Consent, Personal Data Breach, Data Concerning Health, Cross-Border Processing, Supervisory Authority, Special Categories of Data, Data Subject, Appropriate Technical and Organisational Measures, Data Minimisation, Accuracy, Storage Limitation, Integrity and Confidentiality, Accountability, Joint Controllers, and Data Protection Impact Assessment shall have the meanings given to the terms in the GDPR (2016/679).

Privacy Notice / Privacy Statement shall mean the public statement or notice published by an organisation which describes what data they collect about individuals, how and why this data is processed, and what other organisations they share this data with.

Special Categories of Personal Data under the GDPR, "personal data relating to criminal convictions and offences" under the GDPR; "personal data kept for, or obtained in the course of, the carrying out of social work by a public authority, public body, a voluntary organisation or other body" (Data Protection Act 2018)"; or data relating to judicial proceedings (e.g. court order). In addition, University of Galway treats as sensitive data electronic communications data, employment data and financial data.

Sub-Processors shall mean any person or legal entity which is not party to any Contract(s)/Agreement(s) between the University of Galway and a Service Provider and which is engaged by a Service Provider to perform any or all of its obligations in relation to the Processing of University of Galway Personal Data, including for the avoidance of doubt, a Service Provider group company including subsidiaries and affiliates.

Surveillance means:

- monitoring, observing, listening to or making a recording of a particular person or group of persons or their movements, activities and communications, or
- monitoring or making a recording of places or things by or with the assistance of surveillance devices.
- Surveillance device means an apparatus designed or adapted for use in surveillance, but does not include:
    - an apparatus designed to enhance visual acuity or night vision, to the extent to which it is not used to make a recording of any person who, or any place or thing that, is being monitored or observed.
    - a CCTV within the meaning of section 38 of the Garda Síochána Act 2005.
    - a camera, to the extent to which it is used to take photographs of any person who.
    - anything that, is in a place to which the public have access.

University of Galway (UoG) premises means the buildings or lands located (i) on the main campus located at University of Galway, University Road, Galway, Ireland H91 TK33, its environs both internal and external, and (ii) includes any premises and associated environs both internal and external as may be leased or owned by the University of Galway on a permanent, semi-permanent or temporary basis, (iii) all satellite site locations and associated environs both internal and external including substantially adjacent or proximal to the main University of Galway campus and (iv) outreach or remote locations including environs both internal and external as may be operated by the University from time to time.

Video still - When a still is produced by saving one frame to evidence lock for future investigation. The retained duration will be determined by the investigation needs as with CCTV footage.

Video snippet – When a small piece or brief extract is retained from a piece of CCTV footage.

Appendix 2
Body Worn Cameras (BWC)

BWC User is the individual (typically a security guard) operating the BWC. For the avoidance of doubt, it is the individual that activates recording via the BWC.

BWCs are used to capture an interaction or a series of interactions between the BWC User and other individuals. Typically, BWCs are removably attached to the users clothing. The primary Users of BWC are University of Galway security staff members and contracted security staff members.

Scope

The protocols regarding BWCs apply to all users of BWCs on University of Galway premises, and all users who have access to BWCs and footage obtained therefrom.

Objectives

BWCs are used for a range of operations across the University of Galway premises. They are used for purposes that align to those of CCTV. However, there are specific purposes that are specific to BWCs as follows:

- Raise standards of security staff during confrontational incidents.
- Act to dissuade and reduce incident escalation(s).
- Reduce complaints.
- Reduce false accusations.
- Protect individuals, both Users and other individuals as may be encountered when the device is switched on.
- For health and safety purposes.
- Augment footage and audio evidence.
- Assist with University of Galway disciplinary proceedings for staff and/or students, noting we will not use it for performance or attendance.
- Assist in legal proceedings taken by or actions taken against University of Galway.
- Assist in regulatory investigations by appropriate regulatory authorities including but not limited to the Health and Safety Authority.
- Assist staff to enter Student Accommodation, where it is mandatory to use BWCs for reasons of welfare.

General Principles

All personal data captured on BWC's is personal data as defined by the Data Protection Act, 2018 and the GDPR.

University of Galway is the Data Controller where it is the sole operator for all data processed and or captured by the BWCs.

The Security Services Supervisor is primarily responsible for the operation and ensuring that BWCs protocols are followed by Security Officers.

All security staff issued with BWCs are responsible for the operation of their equipment and BWCs, including providing justification for switching on a BWC and determining the risk for same.

All security staff to receive targeted trainings on the use of BWCs in accordance with the University of Galway CCTV and Data Protection policies and procedures to include BWCs and ANPR.

Managers and supervisors of University of Galway premises will be responsible for ensuring all staff with BWC are operating same using a risk assessment based upon their training and in accordance with their assigned duties.

Security Officers on duty use their discretion consistent with their regular CCTV and Data Protection training and only where there is a reasonable expectation of a confrontational incident including but not limited to the threat of violence to the security officer or to other person(s) or themselves on University of Galway premises. BWCs are mandated for all entry into student accommodation apartments or rooms.

Security staff must take all possible steps to ensure the confidentiality of footage.

University of Galway asserts its ownership and copyright of all data, footage and material recorded via CCTV/BWC/ANPR systems.

Misuse

Any breach of these protocols including but not limited to confidentiality breaches, copying by any means, disclosure to unapproved person(s) including displaying footage to unauthorised persons, sharing via any means or the covert use of BWCs are dealt with in accordance with established University of Galway disciplinary procedures or through Supplier Agreements as applicable.

BWCs should not be 'always on'. Further 'always on' capture on a BWC is classified as a misuse and may be subject to disciplinary action.

BWCs should not be deactivated during an incident or actions to stop recording, obscure, cover, hide, or alter the field of vision, alter or supress audio of a BWC during an incident whether such actions are deliberate or not are classified as a misuse and may be subject to disciplinary action.

BWCs should not be deactivated to protect colleagues' infractions of this policy or misuse, such actions are classified as a misuse and may be subject to disciplinary action.

BWC should not be damaged by the User and may be classified as a misuse and may be subject to disciplinary action.

BWCs should not be used covertly, any use of BWCs used covertly is classified as a misuse and will be subject to disciplinary action.

Protocol for using BWCs

- BWCs will be operated in accordance with the protocols set down in this Appendix to the CCTV policy.
- All users of BWCs at University of Galway are to receive a copy of the CCTV policy and the appendices for BWCs and in accordance with the functions of their role and the permission level authorisation assigned to them. BWC users must be fully aware of the contents of these documents contents, and he/she are mandated to comply with these policies and protocols at all times.
- Users of BWCS are to ensure that they have completed the training in BWCs provided by the University or its nominated provider.
- Users must contact the control centre when they anticipate the requirement for recording using their or other security members BWC. They must inform the controller that he/she is about to record an incident and explain details of their reasons for same. The Controller must log the details including the Date and timestamp, BWC user ID and location as well as any other relevant details in the BWC log.
- To ensure fair processing users of BWCs prior to switching on a BWC must ensure that person(s) are informed verbally via plain language statements and ensuring that the verbal warning is of sufficient

volume as to be clearly heard by individuals in the immediate vicinity that the camera will be recording. Where audio is recorded this must also be clarified.

- The BWC User must state clearly why the BWC recording is being activated. They should state the date time and location, nature of the incident so that individuals are aware and know that the recording is active. Where audio is recorded this must also be clarified.
- Where a BWC does not have a clear recoding light or indicator the user must wear the University issued badge, which badge has the following text in clear bold font stating Body Worn Video recording in progress and attention must be drawn to the badge text prior to turning on the BWC. Where audio is recorded this must also be clarified.
- BWCs should not be activated where there is an elevated expectation of privacy e.g. dwelling places, residence(s) or toilets.
- Where a User anticipates the requirement of the activation of a BWC they must seek permission from the Supervisor and provide details and a rationale of the risk to the Controller on duty. Only in exceptional circumstances should BWCs be activated for example where there is a treat to life, or serious injury to individuals, children or vulnerable persons. Where BWCs are approved for use in such circumstances they should be strictly limited to record only what is necessary and proportionate.
- The decision to record or not record is the responsibility of the BWC user. For the avoidance of doubt all incidents that normally require reporting, if a BWC not present, should be recorded.
- The Security Services Supervisor is responsible for regularly auditing BWCs. Audits may be in the forms of spot checks, and/or examination of the BWC and any storage or image/video/audio content stored on the BWC.

Protocols for recorded data

- All access to BWC footage by Data Subjects is by the Data Subject Access Procedure identified in the CCTV policy and in the QA444 Data Subject Rights Request Procedure
- All access to BWC footage by Law Enforcement bodies is in accordance the Section 41 of the Data Protection Act, 2018 access process identified in the CCTV policy.
- BWC footage is auto saved to the hard drive on the device and retained for as long as the capacity of the drive is available which can vary. New footage will overwrite oldest footage when capacity has been reached. In the event of footage being required for an investigation or other, the section of footage needed will be downloaded from the device to a security local hard drive and secured for the duration requested or delated if requested to do so by the Supervisor, Security Services.
- When BWC footage is required for an investigation and needs to be downloaded to a portable or external device, this is done by encryption through the CCTV software system with a generated password. For external devices, the encryption code will be sent to the applicant through e mail or text independently from the storage device. The security will not retain the unique code for unlocking the encryption.

Video snippets/stills

A snippet of video/still or audio which is stored on a BWC or on University of Galway computer device or computer media are not taken routinely.

Details of a snippet must be entered into a log having at least the following information:

- The name and ID of the security officer making the snippet.
- Confirmation that the security officer has permission authorisation to access the footage.
- The time and date of the making of the snippet.

- The purpose for the snippet.
- The justification for making the snippet.
- The full details and circumstances under which the snippet is taken e.g. as part of a DSAR, S 41 request by Law Enforcement bodies, internal University of Galway investigation etc.
- Approval from the Security Services Supervisor must be sought prior to the disclosure of a snippet.
- The Security Services Supervisor or their appointee maintains a record of the snippet in a log.
- Retention period.
- The period of retention will be determined at the time of the downloading and will be delated on request by the Supervisor, Security Services when the snippet is no longer needed or part of an investigation.

Appendix 3

Automatic Number Plate Recognition (ANPR)

For the avoidance of doubt, ANPR tracks all vehicular entry and exits captured on the University ANPR cameras. This includes vehicle registration/number plates. Footage is retained a maximum of 1 month, unless specifically required for investigation/ security/safety/legal purposes, in accordance with Record Retention Policy (QA442) and Record Retention Schedule and Guidance (QA442).

The Automatic Number Plate Recognition (ANPR) CCTV deployment captures car registration details only, and there is no automated matching of data to any National or EU number plate database for example the National Driver Licence Service (NDLS) database or vehicle checking websites.