Maynooth University
Data Protection Office and
Campus Services

CCTV Policy

POLICY IN RELATION TO THE OPERATION OF CLOSED CIRCUIT TELEVISION CAMERAS IN MAYNOOTH UNIVERSITY

Author / Policy Owner:	Campus Services
Creation Date:	12th September 2018
Review Date:	31st August 2022
Next Review Date	**30th September 2025**
Version:	1.1
Scope:	This policy applies to all staff, students and members of the public who use the Maynooth University Campus
Approved by UE Date:	**24th January, 2023**

Revision History

Date of this revision: 31st August 2022	Date of next review: 30th September 2025

Table of Contents

1. Introduction

Maynooth University is committed to providing a safe environment by integrating the best practices of security management with state of the art technology. A critical component of the University's Security Management System is Closed Circuit Television (CCTV), a technology that can remotely monitor and record activity on campus. The use of CCTV at Maynooth University has expanded rapidly since the mid-1990s. The need for recognised standards and safeguards has also developed over this time. There is a need for the University to ensure accountability, together with a good quality, effective and well managed system.

The purpose of this Policy is to provide guidelines to regulate the management, operation and use of the CCTV systems in Maynooth University (hereafter referred to as "the University") in a way that enhances security whilst respecting the expectation of reasonable privacy among members of the community (i.e. staff, students and visitors).

This Policy is informed by the principles set out in the General Data Protection Regulation (GDPR), Data Protection Law and the Freedom of Information Act 2014 together with guidance issued by the Office of the Data Protection Commissioner 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, (hereafter referred to as the Garda Code of Practice). This Policy will be kept under review with regard to the system meeting its purposes.

University entities using CCTV monitoring are responsible for implementing this Policy, including the Operational Code of Practice, in their respective Departments, Buildings, Units or areas.

2. Background

Systems to ensure the safety of staff, students and visitors and the protection of property have been in operation in the University for over 18 years and the systems employed have developed significantly over that time. CCTV is now an integral part of the Security Management Systems employed by the University and we have in recent times moved from analogue to digital systems and extended our coverage of the campus.

The CCTV systems installed have the primary purpose of protecting University premises and helping to ensure the safety of the University's community consistent with respect for the individuals' privacy. They also aid in reducing the threat of crime generally. These purposes will be achieved by monitoring the systems to:

- deter those having criminal intent
- assist in the prevention and detection of crime
- facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order offences
- facilitate the identification of any activities/events which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to management and/or to a member of staff or student against whom disciplinary or other action is being, or is threatened to be taken.
- facilitate the movement of vehicles on site.
- in the case of security operatives to provide management information relating to compliance with contracts of employment / engagement.

The system will not be used:

- to provide recorded images for the world-wide-web.
- to excessively monitor the students, staff and visitors to the campus and buildings. Recording and monitoring of persons on the campus will be limited to that which is necessary to achieve the purposes set out above.
- to record sound except in the case of the personal camera systems

3. Code of Practice for CCTV Systems in Maynooth University

University security management incorporates various CCTV systems managed by different entities and comprised of different types of cameras and recording equipment. Throughout this document, any reference to "CCTV" shall include a reference to any or all of these systems.

The existence of this Policy does not imply or guarantee that cameras will be constantly monitored in real time and whilst security management planning and design endeavours to ensure that the CCTV systems will give maximum effectiveness and efficiency, it is not possible to guarantee that the systems will cover or detect every single incident taking place in the areas of coverage.

All existing uses of video monitoring and recording shall be brought into compliance with this Policy within 12 months of the approval of this Policy.

3.1. Main Campus CCTV System

The main campus CCTV system comprises of internal and external CCTV cameras located around the campus which are streamed to a platform in the security office in the John Hume Building and to the security hut on the south campus from where they can be monitored. These cameras are both fixed and pan tilt zoom cameras.

The cameras provide general coverage of the public access areas of the University and are used to monitor building access and egress points.

These cameras are all on a dedicated security network linked back to Campus Security. In the case of some user operated buildings the images relating to that building can be reviewed locally by the Manager of that building.

3.2. Local CCTV System

Some user operated buildings and some of the Licensees on campus operate their own CCTV systems to secure their area. The main construction sites on campus also typically utilize CCTV to protect their site area. These systems are typically fixed cameras to address a specific risk. These users will all be made aware of this policy and be expected to adhere to its operating guidelines.

3.3. Campus Residences CCTV System

Student residences' CCTV system comprises of internal and external CCTV cameras located around the residences. External cameras cover the access routes to the residences and general circulation areas, the internal cameras monitor the main entrances into each house. This system is managed by Campus Security

3.4. Security Personnel Personal Systems

Security personnel can sometimes have to deal with volatile or aggressive situations and for this reason some security personnel are issued with a personal body worn CCTV camera and recorder. The camera is activated by the security operative as required and footage including audio is downloaded to record incidents. Personal systems shall be owned and managed by Maynooth University or its agents and the resulting data shall be owned and managed by Maynooth University or its agents.

The use of these body worn cameras will be restricted to situations where there is actual or likely damage, injury or aggression. Recordings including audio will be deleted where they are not required for evidential purposes. Body Worn Camera Protocols & Guidelines is available as a separate document.

3.4.1 Audio

Audio recording and 'Privacy by Design' for GDPR, have been incorporated within the Policy and operational applications:

(a) Audio Data collection will be limited to incidents outlined in the Body Worn Camera Protocols & Guidelines.

(b) Security Control of the system is per this CCTV policy – sections 5, 6 & 7.

(c) Access Control of the data is per this CCTV policy - section 8.

(d) Process Monitoring is in place with quality assurance by the General Services Manager

3.5. Covert recording

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance shall only be permitted on a case by case basis where the data is kept for the purposes of preventing, detecting or investigating offences or apprehending or prosecuting offenders. This provision automatically implies an actual involvement of An Garda Síochána or an intention to involve An Garda Síochána. Covert cameras may be used under the following circumstances on the written request of security and where it has been assessed and approved by the Director of Campus and Commercial Services as the relevant Data Protection Officer

- that informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and

- that there is reasonable cause to suspect that illegal activity is taking place or is about to take place and the recording will assist in preventing, detecting or investigating such illegal activity.

Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal activity.

The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

Throughout this document, any reference to "CCTV" shall include a reference to any or all of the above systems.

4. Principles Governing the Operation of CCTV Systems in Maynooth University

4.1. Compliance

The University's use of CCTV systems confers a duty on it as an organisation to keep personal details private and safe. The University as the organisation who controls the contents and use of personal details is known as the "Data Controller". As a Data Controller the University has responsibilities in the handling of personal details consisting of photographs or digital recordings of a person's image or recordings of their voice. The University will treat the systems and all information, documents and recordings obtained and used, as data which are protected by the Data Protection and Freedom of Information Acts.

All CCTV systems operating in the University must operate in compliance with:

- Current legislation covering Data Protection and Freedom of Information as well as guidance issued by the Office of the Data Protection Commissioner or the Office of the Information Commissioner if applicable.

- The Garda Code of Practice which represent best practice in relation to CCTV systems in Ireland. The full text of the Garda Code of Practice is available at: https://www.gov.ie/en/publication/8fc2d-code-of-practice-for-community-based-cctv-systems/

- Additional requirements drawn from the UK Code of Practice for CCTV.

4.2. Purpose

The main purpose of CCTV systems in the University is to assist the following in a proportionate manner:

- the safeguarding of the personal safety of all persons on campus;
- the safeguarding of campus property;
- the maintenance of security on campus;
- the facilitation of proceedings in the context of criminal or legal issues; and
- the investigation of staff or student disciplinary offences under University policy or student code.

CCTV may also be used for purposes other than security, e.g., as part of a research project, for the purpose of recording the progress of a large building project or for monitoring the performance of important items of equipment or machinery.

4.3. Signage

Signs will be prominently placed at strategic points at entrance and exit points of the campus and in buildings; to advise staff, students, visitors and members of the public of the presence of the CCTV system, save where covert cameras are required on an exceptional basis. These signs will indicate the purpose for which the system is being used (i.e. for safety and security)

5. Data Controller

Data Protection Law require that a Data Controller be appointed to manage and control data generated as a result of the operation of CCTV systems to ensure compliance with the Acts. The Data Controller for each of the University systems is as follows:

System	Data Controller	Contact
Main Campus System	Maynooth University	General Services Manger
Local CCTV System	Maynooth University	Local Buildings Manager or Head of School
Campus Residences CCTV System	Maynooth University	General Services Manger
Security Personnel Personal Systems	Maynooth University	General Services Manger
Covert Systems	Maynooth University	Director of Campus and Commercial Services

6. Operation of CCTV Systems

In the operation of CCTV systems, the University will have the greatest possible regard for the protection of the fundamental right to privacy enjoyed by the University community (staff and students and visitors), and their rights of free association and free expression within the law.

Those charged with the operation of the various CCTV systems in College will exercise care to ensure that the systems are not used in any unauthorised or inappropriate manner. This policy has been drafted with the principles set out in the General Data Protection Regulation and Data Protection Law in mind and CCTV will only be used where it is a proportionate method to protect persons and property.

CCTV cameras will not be used with the intention of monitoring or recording student union or trade union activities in the University.

All recorded CCTV footage must be adequately secured and access to footage must be password-controlled.

6.1 Monitoring
Cameras shall only cover areas intended to be covered by the system[1]

Camera control operators will NOT view private rooms or areas through windows.

Monitoring will be conducted in a manner consistent with all existing University policies, including the Non-Discrimination Policy, the Sexual Harassment Policy and other relevant policies. Monitoring based on the characteristics and classifications contained in Equality Regulations is strictly prohibited.

Unless an immediate response to events is required, staff in control of CCTV will not direct cameras at an individual or a specific group of individuals.

6.2. Staff
CCTV monitoring will be conducted in a professional, ethical and legal manner. All staff working with CCTV will be made aware of the sensitivity of handling CCTV images and recordings. The Operations Room Manager and his/her nominee(s) are authorised to operate and monitor the CCTV system. Such nominees must be authorised in writing by the Operations Room Manager and a record of such authorisation be maintained by the Operations Room Manager. The Operations Room Manager will ensure that all staff are fully briefed and trained in the technical, legal and ethical parameters of appropriate camera use.

Authorised personnel are responsible for ensuring that the system is only used in an appropriate manner in conformance with legislative and any legal requirements that may arise. All operators should be aware of the procedures in relation to the Data Protection Acts. Training in the requirements of the Data Protection Acts, relevant guidelines and this Policy and Code of Practice will be given to all those required to work with CCTV. Camera control operators will receive a copy of this Policy and provide written acknowledgement that they have read and understood its contents.

All operators and supervisors involved in CCTV surveillance will perform their duties in accordance with this Policy.

Violations of the Code of Procedures may result in disciplinary action consistent with the rules and regulations governing employees of the University.

Therefore, operators of the cameras should be aware of the purpose of the cameras and only use them for that purpose.

Staff operating the systems should be able to explain to members of the public the type of images which are recorded and retained, the purposes for which those images are recorded and retained, and information about the disclosure policy in relation to those images.

7. Recording

The signals received from the cameras on the Campus system and the internal building systems are recorded on digital video recorders (DVRs) or network video recorder (NVRs) and the recordings are retained on the DVRs/NVRs for a period of time, usually between fourteen and thirty one days after which they are automatically erased. The length of time that recordings are stored varies depending on the capacity of the DVR/NVR hard disk and the number of cameras connected to the particular system. The principle is adopted that if recordings do not produce relevant images then they should be deleted, or recorded over, within 31 days.

Where relevant images are produced and are required in relation to an incident the recording shall be burned onto a CD and be retained securely by the Data Controller and a second copy will be handed over to the recording requestor as provided for under this Code of Practice.

All hard drives and recorders shall remain the property of Maynooth University until disposal and

[1] Point 2.1, Siting Standards, Code of Practice for CCTV Systems authorised under Section 38(3)(C), Garda Síochána Act 2005.

destruction.

8. Retention of CCTV Footage

In accordance with GDPR and Data Protection Law, CCTV footage is retained for no longer than is necessary. In general, footage will only be retained for a period of fourteen to thirty one days unless valid reasons including those set out in section 4.2 above arise.

8.1 CCTV Footage retained as evidence

The following log of retained recorded CCTV footage will be maintained by the Operations Room Manager or his/her nominee(s):

- the date and nature of the matter recorded;
- the date(s) and timeframe(s) of when the CCTV footage was copied;
- record of any disclosure of CCTV footage;
- record of when and how the CCTV footage was securely deleted.

CCTV footage will be retained for as long as required where it serves as evidence of matters such as those set out in section 4.2 above, as identified by the Operations Room Manager or his/her nominee(s).

In the event that CCTV footage is to be retained the following procedure shall apply:

- the relevant footage will be downloaded onto an appropriate secure storage device by the Operations Room Manager or his/her nominee(s) and retained in a secure location;
- the copy will be securely retained until written confirmation from the relevant University manager is received to confirm that the matter is concluded. Upon receipt of such confirmation, the footage will be securely erased by the Operations Room Manager or his/her nominee(s).

Hard copy versions of CCTV footage are subject to the same requirements as those set out above.

9.Secure storage of CCTV

DVR's/NVR's storing the recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel.

10. Access to CCTV Recordings

Access to images will be restricted to those University staff or agents who need to have access in accordance with their role and with the purposes of the system.

10.1 Access to images by third parties
Recorded material containing personal data will only be released to third parties in the following circumstances and processed by the General Services Manager or Director of Campus and Commercial Services:

- A formal request from a member of An Garda Síochána (Rank Sergeant or above**)** for disclosure of images, on the grounds that the images are likely to be of use for the investigation of a particular offence;
- A requirement under any enactment, rule of law or court order to disclose the images;
- Where a valid data access request is made by an individual under Data Protection Law; or
- Where in rare circumstances the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime. The release of images to the media in a criminal investigation is solely within the remit of An Garda Síochána.

In the above circumstances, the original copy shall be retained by the Data Controller and a copy provided, unless needed for court proceedings or under an Act. The following should be documented,

i. The date and time of the removal.

ii. The name of the person removing the images.

iii. The name(s) of the person(s) viewing the images. (If this should include third parties, the name of the organisation to which the third party belongs).

iv. The reason for the viewing.

v. The outcome, if any, of the viewing.

vi. The date and time the images were returned to the system or secure place, if they have been retained for evidential purposes.

10.2 Access to images by a subject
CCTV digital images, if they show a recognisable person, are personal data within the meaning of the General Data Protection Regulations. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in Data Protection Law. They do not have the right of instant access.

A person whose image has been recorded and retained and who wishes access to the data must apply in writing or email to the University Data Protection Officer dataprotection@mu.ie. Data Access Request Forms are obtainable from the security office. The Data Controller will endeavour to locate the images when requested and determine whether disclosure of the image would involve disclosing the images of third parties, if so, arrangements will be made for those images to be disguised or blurred and which may require engaging another party or a company to carry out that type of editing subject to guarantees regarding security measures in relation to the images.

The Data Protection Officer will then arrange for a copy of the data to be made and given to the applicant. A response will be provided promptly and in any event within twenty days.

The GDPR and Data Protection Law gives the Data Protection Officer the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

10.3 Access Log

If access is sought pursuant to section 10.1 or 10.2 the following log to record such access will be maintained by the Head of Security or his/her nominee(s):

- the date the access was granted;
- the name and details of the person who sought access;
- the dates(s) and timeframe(s) of the CCTV which was accessed;

11. Enquiries

The contact point for members of the university community or members of the public wishing to enquire about the CCTV system will be the:

General Services Manager, Campus and Commercial Services
Phone (01) 474 7781
Email ivan.griffin@mu.ie
Education House Building, North Campus.

Upon request, enquirers will be provided with:

A Copy of this Statement of Policy
Further information on the GDPR and Data Protection Law is available at
https://www.maynoothuniversity.ie/data-protection