

Closed Circuit Television (CCTV) Policy

Version 1.0

16th June 2026

Document Details	
Document Title:	Closed Circuit Television (CCTV) Policy
Version:	1.0
Approved By:	Governing Body
Date Approved:	16 th June 2026
Effective Date:	16 th June 2026
Review Date:	15 th June 2029
Policy Owner:	Chief Operations Officer

Consultation Details	
Name:	Draft policy was discussed with a number of parties including Data Protection Office, Senior Vice President – Chief Operations Officer, Estates Offices, Unions
Date:	2025/26
Details of Consultation	Consultation with Staff Representatives took place in January and February 2026

Revision History		
Previous Version No.	Summary of Amendments	Version No.
N/A	First draft	0.1
0.1	Draft following consultation	0.2
0.2	Reviewed by Policy Committee 11th June 2026, minor amendment and recommended for approval by Governing Body	0.3
0.3	Approved by Governing Body 16th June 2026	1.0

Publication Details	
SETU Website	
Drive/Public/HR/Policies	
All Staff Email	

Feedback or issues arising on implementation of this policy should be communicated to the policy author.	
Policy Author:	Estates Managers

Policy Management Framework Compliance Review as requested by EMT all draft policies should be reviewed by the Policy Review Group ¹ in advance of review by EMT. Please confirm that the policy was reviewed by the policy review group.	
Date Policy Reviewed:	30 August 2023

¹ Contact susan.green@setu.ie or michelle.farrell@setu.ie

Contents

1. Introduction/Context	1
2. Purpose of CCTV Policy	1
3. Scope of CCTV Policy	1
4. Principles Governing the Operation of CCTV	2
5. Definitions	4
6. Policy	5
7. Compliance.....	7
8. Responsibility and Authority	7
9. Related Documents.....	8
10. Review of Policy	8

1. Introduction/Context

This Policy sets out the University's approach regarding the use of Closed-Circuit Television (CCTV) systems.

This Policy document compiles with Irish Law (Data Protection Acts, 1988, 2003 and 2018) and European Law (Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR). The Policy highlights certain legal obligations set down in the Data Protection Acts, EU Regulations and the SETU Data Protection Policy <https://www.setu.ie/data-protection>.

2. Purpose of CCTV Policy

The purpose of CCTV at SETU is to support the safety and security of the University community and the protection of University property. CCTV systems are operated in a proportionate manner and only for legitimate operational purposes consistent with this policy and applicable data protection legislation.

CCTV systems are used for the following purposes:

- Supporting the prevention, deterrence, detection and investigation of criminal activity, security incidents and anti-social behaviour
- Supporting the safety and wellbeing of staff, students, contractors, visitors and members of the public
- Protecting University buildings, facilities and assets
- Assisting in the investigation of reported incidents
- Providing evidential material to An Garda Síochána and other statutory bodies where lawfully requested
- Supporting University security management and incident response procedures

CCTV will only be used for the purposes outlined in this policy. It will not be used for any unrelated purpose.

CCTV monitoring is conducted using overt systems. Cameras are positioned in visible locations where possible and appropriate signage is displayed to inform individuals that CCTV is in operation in accordance with transparency obligations.

The University does not use CCTV for routine monitoring of staff or students. Any access to footage relating to individuals will only occur where necessary for the investigation of a specific safety, security or disciplinary incident and in accordance with University procedures.

3. Scope of CCTV Policy

This policy applies to all CCTV systems owned, leased, managed or operated by SETU across all University campuses, properties and facilities.

The policy governs the operation, management and use of CCTV systems including the monitoring, collection, recording, storage, retrieval, viewing, disclosure and deletion of CCTV footage in accordance with applicable data protection legislation.

This policy applies to:

- All locations where CCTV systems are installed by or on behalf of SETU
- All SETU staff involved in the management, operation or oversight of CCTV systems
- Authorised third parties acting on behalf of SETU (Data Processors)

- All individuals whose personal data may be captured by CCTV systems including staff, students, contractors, service providers, visitors and members of the public

This policy does not apply to:

- Personal recording devices not operated on behalf of SETU
- CCTV systems installed by third parties not acting under SETU authority (except where SETU is the Data Controller)
- Recordings made for journalistic purposes or by law enforcement bodies operating under their own statutory authority

SETU acts as the Data Controller for CCTV systems within the scope of this policy and will ensure that such systems are operated in a lawful, fair and transparent manner consistent with the University's obligations under the General Data Protection Regulation (GDPR) and the Data Protection Acts 2018–2022.

This policy should be read in conjunction with SETU's Data Protection Policy, Data Retention Policy, and any relevant IT and Security policies.

This policy will be published on the SETU website and made available to staff, students and the public.

4. Principles Governing the Operation of CCTV

SETU operates CCTV systems in accordance with the following core principles to ensure their use is lawful, proportionate, transparent and consistent with the stated purpose of supporting safety and security.

Lawfulness, Fairness and Transparency

CCTV will be operated in a lawful, fair and transparent manner in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Acts 2018–2022.

The University will ensure individuals are informed of CCTV through appropriate signage and the publication of this policy.

Purpose Limitation

CCTV systems will only be used for the safety and security purposes outlined in this policy.

CCTV will not be used for purposes unrelated to security and safety. Footage will only be reviewed where necessary for the investigation of a specific incident or legitimate operational requirement.

Necessity and Proportionality

CCTV will only be installed where there is a demonstrable safety, security or operational risk and where CCTV is considered a necessary and proportionate control measure.

Camera locations and coverage will be limited to what is required to achieve the stated purpose and will avoid intrusion into areas where there is a reasonable expectation of privacy.

Duty of Care and Safety Obligations

SETU operates CCTV systems as part of its duty of care obligations under the *Safety, Health and Welfare at Work Act 2005* to support a safe environment for staff, students and visitors.

CCTV forms one element of the University's overall security and safety arrangements.

Governance and Authorisation

CCTV systems may only be installed, altered or expanded following appropriate approval in accordance with University governance procedures.

No CCTV system may be installed on SETU premises without formal authorisation from the designated University authority (normally the Estates Manager or equivalent governance structure).

Controlled Access

Access to live feeds and recorded footage will be restricted to authorised personnel with a legitimate operational need.

Access, use and disclosure of CCTV recordings will be controlled and recorded in accordance with University procedures and data protection requirements.

Data Protection and Accountability

CCTV recordings which identify individuals constitute personal data and will be processed in accordance with data protection legislation and University policies.

SETU will ensure appropriate oversight, management responsibility and accountability arrangements are in place for the operation of CCTV systems.

Retention and Disposal

CCTV footage will only be retained for as long as necessary for security and operational purposes and will be securely deleted in accordance with the University's retention requirements (Section 6.5) unless required for an active investigation.

5. Definitions

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy:

Access Request	This is where a person makes a request to the organisation for the disclosure of their personal data under Article 15 of the GDPR.
Authorised SETU Personnel	For the purpose of this policy authorised SETU personnel include SETU Estates Managers & Approved Estates Staff Members.
CCTV	A system of digital cameras used to monitor and record images for safety and security purposes, with recordings stored on secure digital systems and processed in line with data protection legislation.
Data Controller	Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, Processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
Data Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Processor	Means a person or organisation that holds or processes Personal Data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the Personal Data. An employee of a Data Controller, or a School or Function within SETU which is processing Personal Data for SETU as a whole, is not a Data Processor. However, someone who is contracted by the Data Controller to provide a service that involves the processing of Personal Data would be a Data Processor. It is possible for one SETU or person to be both a Data Controller and a Data Processor, in respect of distinct sets of Personal Data. It should be noted however that, if you are uncertain as to whether SETU is acting as a Data Processor or a Data Controller of Personal Data, it should be treated as being the Data Controller (and therefore comply with the Data Protection Policy in full).
GDPR	Means EU regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the processing of Personal Data and on the free movement of such Data which was adopted into Irish law in May 2018.
Internal area	An "internal area" typically includes common areas such as lobbies, corridors, reception areas. It also may include rooms and sheds where goods and stock are held. This list is not exhaustive.
Personal Data	Means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

6. Policy

6.1 Access

In relevant circumstances, CCTV footage may be accessed:

- By authorised SETU Personnel (please see definition section);
- By third party security companies (known as Data Processors) retained by SETU to operate CCTV and other security functions;
- Following a lawful request by An Garda Síochána;
- By an Insurance Company acting on behalf of SETU.

Information obtained through CCTV monitoring may be downloaded from the system only when authorised by the Data Protection Office.

6.2 Request for Access

6.2.1 Individuals

Individuals have the right to access their personal data including their image in CCTV recordings. Requests can be made using the link below:

[Data Protection Subject Access Request \(SAR\) Application Form \(cognitoforms.com\)](https://cognitoforms.com)

SETU will not release CCTV footage to staff, students, or other third parties where other individuals are identifiable in the recording. In accordance with GDPR and the Data Protection Act 2018, the University must protect the rights and privacy of all individuals captured on CCTV. Although data subjects have the right to access footage in which they appear, this right does not extend to images that would disclose the identity of others.

Where possible, SETU may consider redaction to obscure third-party identities before any footage is released. If effective redaction cannot be achieved, the University may be unable to provide the requested footage.

Individuals who believe that a criminal offence has occurred should report the matter to An Garda Síochána. Gardaí may request relevant CCTV footage directly from the SETU Data Protection Office as part of an official investigation.

6.2.2 An Garda Síochána and other requests

All requests from An Garda Síochána for access to CCTV footage or other personal data must be submitted in writing to

dpo@setu.ie and must be authorised by a senior Garda officer. This enables the data controller to verify the legitimacy and lawfulness of the request under GDPR and the Data Protection Act before any disclosure is made.

6.2.3 Access to CCTV for Health & Safety Purposes

Where CCTV footage is required in connection with a health and safety incident or potential or actual litigation, a formal request must be submitted to the Data Protection Officer (DPO).

The DPO will assess the request in accordance with data protection requirements and, where appropriate, will authorise the Estates Department to retrieve, extract and securely retain the relevant footage.

Health and Safety personnel do not have direct or unrestricted access to CCTV systems or recorded footage. Any access will be managed through the above process.

Processing of CCTV data for these purposes is carried out in accordance with applicable data protection legislation, including:

- Legal Obligation (Article 6(1)(c))
- Legitimate Interests (Article 6(1)(f))

6.3 Location of Cameras

CCTV cameras are installed at selected locations across SETU campuses where there is a demonstrable safety, security or operational requirement, and where their use is considered necessary and proportionate to the risks identified.

Camera locations are determined following consideration of security risks, incident history, building use and the need to support the safety of the University community and protection of University property.

Cameras may be located in both external and internal areas including building entrances, circulation areas, public access areas and other locations identified as requiring security monitoring.

SETU will seek to ensure that:

- CCTV coverage is limited to areas where surveillance is necessary to achieve the stated safety and security purposes
- Cameras are positioned to minimise the capture of images outside University property where possible
- Cameras do not intentionally overlook private property or areas where there is a reasonable expectation of privacy
- CCTV is not installed in areas such as toilets, changing facilities or other private spaces

SETU may utilise fixed cameras or cameras with pan, tilt and zoom functionality where operationally required. Such functionality will only be used for legitimate security purposes consistent with this policy.

The University will ensure that the technical specification of CCTV systems is appropriate to the security purpose for which they are installed and is not excessive.

6.4 Notification - Signage

Signage is displayed at appropriate locations on SETU campuses where there is CCTV in operation. Signage shall include details such as SETU contact details and the purpose of the CCTV system.

6.5 Management, Storage & Retention of CCTV Footage

In accordance with data protection legislation, CCTV footage will be retained for no longer than is necessary.

Please note the following:

- All CCTV footage is retained for a maximum of 30 calendar days. The data is automatically deleted after a 30-day period.

- During the 30-day retention period, should a legitimate enquiry be made requesting specific CCTV footage relevant to an investigation, then any relevant footage may be extracted and retained as evidence pending an investigation / prosecution.

The CCTV recording equipment shall be securely stored by the Estates Office. Unauthorised access to the CCTV Control room is not permitted at any time.

7. Compliance

It is expected that all employees of the University will comply with this policy.

8. Responsibility and Authority

8.1 Governance Oversight

Overall governance oversight of the University CCTV framework rests with the Senior Vice President / Chief Operations Officer, who has responsibility for ensuring appropriate governance arrangements are in place for the operation of CCTV systems.

8.2 Operational Responsibility

The Estates Managers on the relevant campuses are responsible for the implementation and operational management of CCTV systems in accordance with this policy. This includes oversight of installation, maintenance, appropriate use and ensuring systems operate in line with the University's safety and security objectives.

8.3 Data Protection Responsibility

The Data Protection Officer (DPO) is responsible for oversight of data protection compliance relating to CCTV systems. This includes the management of data subject access requests and requests for disclosure of CCTV footage in accordance with data protection legislation and University procedures.

Requests from An Garda Síochána will be coordinated through Estates in consultation with the Data Protection Officer.

8.4 Authorised Users

Only authorised staff may access or operate CCTV systems where this forms part of their official duties. All staff involved in the operation or management of CCTV must comply with this policy and associated procedures.

8.5 Staff Responsibilities

All employees with responsibility for CCTV operation or access must ensure that CCTV systems and recordings are used only for authorised purposes and in accordance with this policy.

Unauthorised access, use or disclosure of CCTV footage is strictly prohibited.

8.6 Non-Compliance

Failure to comply with this policy may result in action under the relevant disciplinary procedures, where appropriate.

9. Related Documents

This Policy should be read in conjunction with other University policies, such as Data Protection Policy.
<https://www.setu.ie/data-protection>

Other related University policies can be found here [SETU Policies](#)

10. Review of Policy

The authors of this policy are the Estates Managers. Any feedback or issues arising on implementation of this policy should be communicated to the policy authors. They are responsible to ensure that the Policy Owner is aware of these comments when reviewing the policy.

This policy will be reviewed in advance of the review date i.e. day month year, and/or as soon as possible following new or updated legislation, national or sectoral policy.