TU Dublin Policy

CCTV Policy

Version 1.0

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH

TU DUBLIN

TECHNOLOGICAL UNIVERSITY DUBLIN

Table of Contents

1. Document Control Summary

Area	Document Information
Author	Campus and Estates and Information Governance
Owner	Head of Campus and Estates
Reference number	
Version	1.0
Status	For Approval
~~Approved by~~ / to be approved by	Governing Body
Approval date	
Next review date	2024
Document Classification	Public

2. Introduction / Context

Technological University Dublin (TU Dublin) currently uses and is further developing Closed Circuit Television (CCTV) to assist in maintaining a safe and secure environment for all the University's staff, students and visitors. CCTV footage may also be used to assist in criminal, legal or internal investigations.

CCTV has been installed in all buildings and on the grounds of TU Dublin (the University). Images are monitored and recorded both centrally and locally in strict accordance with this policy. The system is owned by TU Dublin, managed by the Estates Office and its appointed agents.

Images recorded by CCTV systems are personal data which must be processed in accordance with data protection legislation.

3. Purpose

The purpose of this document is to promote a safe and secure environment for all the University's staff, students and visitors and to clarify the procedure for which the University's CCTV recording and playback system will be used and the timeframe for retention of images.

4. Scope

This policy applies but is not limited to the following, TU Dublin related groups:

- Staff
- Students
- Visitors
- External parties

5. Definitions

For definitions of the data protection terms used in this policy, please see the TU Dublin Common Terms and Definitions document which can be found in the TU Dublin Data Protection Policy.

Incident - is an incident relating to Safety or Security that is deemed to be of such significance that the University has a duty to try to secure evidence for direct action by the University or for submission to An Garda Siochana.

6. Policy Details:

6.1 Policy Overview

This policy is informed by the principles set out in the General Data Protection Regulation (GDPR), Data Protection Act 2018 and the Code of Practice for CCTV Systems authorised under Section 38 (3) (c) of the Garda Síochána Act 2005.
All usage of CCTV other than in a purely domestic context must be undertaken in compliance with the requirements of the Data Protection Acts. Extensive guidance on this issue is available on the Data Protection Commissioner's website at:
https://dataprotection.ie/en/dpc-guidance/guidance-use-cctv-data-controllers
In summary, all uses of CCTV must be proportionate and for a specific purpose. As CCTV infringes the privacy of the persons captured in the images, there must be a genuine reason for installing such a system and such purpose must be displayed in a prominent position.
The CCTV System will be operated fairly, within the law, and only for the purposes for which it was established consistent with respect for the privacy of individuals.

6.2 Policy Details

6.2.1 CCTV System

The CCTV systems may vary from building to building, the system comprises of fixed position and movable cameras, monitors, digital recorders at strategic locations. The cameras cover internal and external areas, entrances, car parks, and perimeters. Signs are prominently placed at relevant areas to inform staff, students, visitors and members of the public that CCTV is in place and that the system is managed by TU Dublin and/or its appointed agents.

6.2.2 Objectives of the CCTV System

The objectives of the CCTV as determined by the Data controller and which form the lawful basis for the processing of data are:

- preventing crime and protecting buildings and assets from damage, disruption, vandalism and other crime,
- the personal safety of staff, students, visitors and other members of the public and to act as a deterrent against crime,
- assisting in day-to-day management, including ensuring the health and safety of staff and others,
- processing of an internal investigation including those investigations leading to disciplinary proceedings.
- assisting in the defense of any civil litigation, including personal injury claims and
- monitoring the security of buildings.

6.2.3 Signage

Signage has been placed throughout the University buildings and grounds to inform users of the University that CCTV is in operation. Signage displays contact details for persons wishing to discuss the processing of CCTV information.

6.2.4 Proportionality

The use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy is difficult to justify, toilets and rest rooms are an obvious example. To justify use in such an area, the Data Controller shall demonstrate in writing to the relevant Head of School/Service Area that a pattern of security breaches had occurred in the area prior to the installation of the system such as would warrant constant electronic surveillance.
Cameras placed so as to record external areas should be positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

6.2.5 Security

TU Dublin and/or its appointed agents are obliged to have appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of the data and against all unlawful forms of processing. Therefore, access controls have been placed on image storage and remote access to live recording is password encrypted.

6.2.6 Covert Surveillance

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on a case by case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders.
The consideration for the use of Covert Surveillance shall only occur following a written request of An Garda Síochána or other prosecution authorities for potential criminal investigation, or where there is a reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.
A request for use will be notified by the Head of Campus and Estates to the Chief Operations Officer and the President. The use of covert surveillance shall be authorised in writing by the President. The Head of Campus and Estates will keep a record of the decision and a written report will be provided to the relevant director and President detailing the Garda request, the nature, duration, and date of cessation of the surveillance including the date of handing over of any material to An Garda Síochána or other prosecution authorities. All surveillance records shall be passed to An Garda Síochána or other prosecution authorities, and any copies destroyed by the Estates Office.

6.3 Records Management and Retention

The Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 2016/679 states that data shall not be kept for longer than is necessary for the purposes for which they were obtained.
Data recorded from CCTV cameras shall be transmitted and stored in a way that maintains its integrity and confidentiality in order to ensure that the rights of individuals whose images recorded by the CCTV systems are protected.

Recorded images will be retained in line with TU Dublin Data Retention Policy and relevant schedules. Following receipt of a valid Request for Access to CCTV, footage may be downloaded and retained in line with the Data Retention Policy and relevant schedules.

6.4 CCTV Access Requests

CCTV is recorded either on a 24-hour continuous or 24 hour non-continuous basis dependant on the camera type. Playback and downloading of CCTV footage is only undertaken in the following instances and in accordance with these Procedures.
Requests for access to CCTV footage must be in line with sections 6.4.1 to 6.4.4 below.

6.4.1 Data Subject Access Requests

Under Article 15 of General Data Protection Regulation 679/16 any person whose image has been recorded has a right to be given a copy of the information recorded. To exercise that right an individual should complete the Data Subject Access Request Form and return it to the Data Protection Office at dataprotection@tudublin.ie.
Please see https://www.tudublin.ie/explore/gdpr/subject-access-request/ for further information and the Subject Access Request Form.
In this instance the University will comply with the request subject to the period in question falling within the retention period for CCTV images.
In such circumstances, the individual should provide precise details of the time to ensure the University can locate the images. They should also provide photographic evidence of themselves. Where the image is of such poor quality as does not clearly identify an individual, that image will not be considered to be personal data. If the footage includes images of other persons, these will have to be redacted unless authorisation is provided by said other individuals, although this may be impractical in a busy public area.

6.4.2 Supply of data to An Garda Síochána

Access requests by members of An Garda Síochána shall be processed where such processing is necessary and proportionate for preventing, detecting, investigating or prosecuting criminal offences. The University must receive a valid request for information by completing the 'Access Request by member of An Garda Síochána' Form, signed by the Garda and Chief Superintendent, confirming Section 41 or Section 70 of the Data Protection Act 2018 and submitted to the Data Protection Office at dataprotection@tudublin.ie or by post to TU Dublin Data Protection Office, TU Dublin, Park House, Grangegorman, 191 North Circular Road, Dublin D07 EWV4.

6.4.3 Other Requests for CCTV Footage

Requests for access to CCTV footage not covered by 6.4.1 and 6.4.2 above from other external parties should be processed via the Head of Governance and Compliance (e.g. for insurance cases).
The disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and data protection legislation.

6.4.4 Incidents

The following procedure applies:

- Where an incident has been reported to Estates via the incident report form, Estates will review available CCTV footage.

- Under no circumstances will Estates allow the complainant to view the CCTV footage.
- Estates will download any CCTV footage relating to the incident in accordance with the University's Data Retention Schedule and forward it to the Head of Governance and Compliance for retention in relation to the incident.
- The complainant will be informed that the saved footage will be kept for a period of time in accordance with the University's Data Retention Schedule and deleted thereafter as per the University's Data Retention Policy.
- Where an incident is captured on CCTV, this data may be used in the process of an internal investigation including those investigations leading to disciplinary proceedings.
- The TU Dublin Incident Report Form is available on the website https://www.tudublin.ie/for-staff/safety-health-welfare/reporting/

6.4.5 Security Control Centre

- Other than Estates staff, access to the Control Centre will be limited to authorised members of senior management, An Garda Síochána and any other person with statutory powers of entry. No unauthorised access to the Security Control Centre (SCC) will be permitted at any time.
- Staff, students and visitors may be granted access to the SCC on a case by case basis and only then on authorisation from the Head of Campus and Estates. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the SCC.
- Before allowing access to the SCC, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organisation they represent, the person who granted authorisation and the times of entry to and exit from the centre. A similar log will be kept of the staff on duty in the SCC and any visitors granted emergency access.
- Details of the administrative procedures which apply to the system will be set out in a Standard Operating Procedures, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.
- As images of identifiable living individuals are subject to the provisions of the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 2016/679, the SCC Supervisor is responsible for ensuring day to day compliance with the legislation. All recordings will be handled in strict accordance with this policy and the procedures set out in the Standard Operating Procedures

7. Related Documents

Outline any related or impacted documents. E.g. the SOP, Standard Operating Procedure required to implement the policy. Include any links where available.

8. Conclusions

Define any summary points and conclusions

9. Document Management

9.1 Version Control

VERSION NUMBER	VERSION DESCRIPTIN / CHANGES MADE	AUTHOR	DATE
1.0	*Amalgamated TU Dublin document*		*May 2020*
1.1	*Review and Update*	*Information Governance Team*	*February 2023*

9.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)

9.3 Document Ownership

Head of Campus and Estates

9.4 Document Review

Detail the process for document review and the cadence of this review.

9.5 Document Storage

List the file location for the latest revision and where in the TU Dublin CMS this is available.

9.6 Document Classification

TU Dublin Public.