TITLE: ***CCTV POLICY***

Effective Date	19 October 2022	**Version**	2
			Changes to bring the Policy in line with current Data Protection Commission guidance; section on covert recording; changes to duties and identities of authorised users; minor changes and restructuring to provide further information and strengthen processes.
Approved By	Management Board	**Date Approved**	19 October 2022
		Review Date	19 October 2027 *or as required*
Superseded or Obsolete Policy / Procedure(s)		**Owner**	
Data Protection Policy (2014-2015)		Facilities Manager and Data Protection Officer (Jointly)	
CCTV Policy (Version 1, 06 February 2019)			
Initial Issue			

1. Purpose of Policy

Carlow College, St. Patrick's (hereafter Carlow College) is committed to providing a safe environment for employees and learners and operates a Closed-Circuit Television (hereafter CCTV) system to support its work in this area.

The purposes of this Policy are to outline:

- What the CCTV system is used for and how it is operated;
- Measures that the College has in place to protect system integrity and security;
- Procedures to ensure compliance with applicable legislation and guidance, including the General Data Protection Regulation (hereafter GDPR), national data protection legislation, and guidance issued by the Data Protection Commission; and
- A clear and best practice approach to the operation of the CCTV system.

This Policy describes various measures connected with use, access to, and disclosure of CCTV images. Given that CCTV images constitute personal data where individuals are identifiable, particular attention has been paid to ensuring that:

- The CCTV system and images are managed in a secure manner;
- Access to the system is controlled, limited and documented;
- The data protection rights of individuals are upheld; and

The College ensures that the use of CCTV in all matters, particularly investigations of any type, including employee and learner disciplinary matters, is lawful, fair, transparent and proportionate. The College operates a CCTV system both inside its buildings and in the grounds. The existence of this Policy does not imply or guarantee that cameras will be constantly monitored, and it is not possible to guarantee that the CCTV system will cover or detect every incident in the areas of coverage.

2. Definitions

The following definitions are taken or adapted from Article 4 of the GDPR:

- **Controller** means the natural or legal person which, alone, or jointly with others, determines the purposes and means of the processing of personal data. Carlow College is the controller of the CCTV system.
- **Processor** means a natural or legal person which processes personal data on behalf of the controller. Netwatch, which provides and monitors Carlow College's CCTV system is an example of a processor. Carlow College has contracts compliant with the GDPR with processors.
- **Personal data** means information relating to an identified or identifiable natural person (data subject).

Authorised user means any user who is authorised to have access to the CCTV system in respect of designated duties, which are outlined in Appendix 1.

3. Scope of Policy

This Policy applies to all persons whose image is captured by Carlow College's CCTV system. This includes, but is not limited to, employees, learners and members of the public visiting the College's premises.

This Policy applies to authorised users who have been designated certain duties in respect of the CCTV system, as described in Appendix 1.

Where the term 'employee' is used in this Policy it is intended to cover all situations where there is an employment relationship, regardless of whether the relationship is based on an employment contract, a volunteer agreement or contract for services etc.

4. Policy Statement

4.1 Purposes of the CCTV System

The purposes for which the CCTV system may be used are:

- To protect the safety and security of persons, property and the premises, and to investigate security incidents;
- To improve and provide information relating to health and safety matters;
- To facilitate investigations into incidents under College policies;

- To facilitate investigations into accidents under College policies;
- Disciplinary matters involving employees and learners of Carlow College;
- To facilitate proceedings in the context of criminal or legal issues.

4.2 Principles governing the operation of the CCTV system

- In the operation of the system, the College has the greatest regard for the protection of the privacy of employees, learners and visitors.
- Carlow College operates the system in compliance with this Policy and the College's Data Protection Policy, the GDPR, the Data Protection Acts 1988 to 2018, the Freedom of Information Act 2014, and relevant guidance, for example, as issued by the DPC.
- The CCTV system is conducted in a manner consistent with all Carlow College policies, including the Equality Policy. Monitoring based on the characteristics and classifications contained in equality laws is strictly prohibited.
- Carlow College processes CCTV in the context of the following GDPR legal bases: legal obligations, contract, and the legitimate interests set out in this Policy.
- CCTV cameras operate on a 24-hour basis, seven days a week. Cameras are a mixture of fixed and pan/tilt/zoom cameras. Each camera covers a designated zone. A camera in the foyer area of Lennon House records on a continuous basis: it is not monitored in real time but footage may be accessed in response to an identified incident.
- Cameras capture images of Carlow College's premises only.
- Cameras will not be installed in areas where persons have a reasonable expectation of privacy.
- Periodic checks are carried out to ensure that cameras are functioning satisfactorily. Maintenance work is carried out in a timely manner.
- Normally, CCTV footage is retained for 30 days. Footage or stills arising from identified incident/accidents may be retained for longer, usually until an incident/accident is resolved, although this will depend on the specific matter.
- Notices are posted at prominent locations on the College premises indicating that a CCTV system is in operation, and provide contact details for queries, save where covert cameras are required on an exceptional basis. See Section 4.8 for further information about covert recording.
- Carlow College will conduct a Data Protection Impact Assessment where changes to its CCTV system are proposed.

4.3 Data security

- The CCTV system supplied by Netwatch is cloud-based and subject to stringent technical security.
- A small number of authorised users have access to the CCTV system in order to permit them to conduct designated duties (see Appendix 1). Authorised users are to use the CCTV system to execute their designated duties only, to exercise the greatest possible care in their use of the system, and ensure that it is not used in an unauthorised or inappropriate manner.

- The CCTV system is available only on the desktop computers of authorised users. Access is controlled by password, which users must ensure is robust. Authorised users are not to share their password with any person.
- Authorised users who are employees must complete the Access Log (template available at Appendix 2) on each occasion they access the CCTV system. The Access Log includes:
    - Name of authorised employee;
    - Date of viewing;
    - Reason for accessing the system / description of incident/accident;
    - Date and time of viewed images;
    - Action taken e.g. view footage.
- The completed Access Log should be sent via email to the Facilities Manager without undue delay. The Policy owners ordinarily have access to the Access Log.
- Copies of recordings or still images will be kept securely, and distributed on a need to know basis only. Where possible, recordings and images are distributed by electronic file sharing permissions or email, and should be password-protected. Removable storage devices (e.g. memory sticks) are to be used in exceptional circumstances only.
- Recordings and stills will be destroyed in a secure manner. Security of recordings and stills is the responsibility of the individual in whose custody they are.

4.4 Processing access requests

All access requests are processed by the DPO. This includes, but is not limited to, requests by:

- Persons whose image is captured by the CCTV system and other valid access requests
- Employees who request footage or stills in connection with the execution of their duties; and
- Members of An Garda Síochána.

The DPO will keep records relating to access requests.

Where an employee wishes to request access to CCTV images in connection with their duties, for example, in connection with an investigation or disciplinary matter regarding an employee or learner, the appropriate employee should discuss this with the DPO. For instance, in the case of a potential disciplinary matter involving an employee, the Human Resources Office is the appropriate department to request access to CCTV images. In a similar situation involving a learner, an employee of the Office of the Registrar should approach the DPO. The DPO will only proceed with an access request where the request is received from an employee charged with responsibility (under their job description or Carlow College Policy) for the incident/accident under review.

The employee requesting CCTV images will be required to certify to the DPO that an incident/accident is being investigated, name known persons, give details of the incident/accident and when (date and time) and where it occurred, including which camera(s) may have captured relevant images. The DPO will request to view the specified images with an authorised employee. The DPO will then liaise with the requesting employee and any other relevant employee (for example, line manager in the case of an

employment matter) and a decision will be made on whether or not to grant access to the CCTV images to the requesting employee for their proposed use. All relevant factors will be taken into consideration in reaching such a decision, including the seriousness of the incident/accident under review. This is to ensure that the use of CCTV is proportionate and fair. The DPO will document this discussion/decision process. If it is decided to grant access, the DPO will provide the requesting employee with any advisable safeguards around the use of the CCTV images. The discussion/decision process described here also applies to authorised users who are employees and are considering using CCTV images in the course of an investigation for which they have responsibility.

In all cases where CCTV images are utilised in a Carlow College investigation or disciplinary matter, the individual concerned will be afforded the opportunity to respond as is imperative under fair procedures.

4.5 Subject access requests

Where a person is identifiable in CCTV images, it constitutes personal data. Individuals have a number of rights, subject to certain exemptions, in terms of their personal data:

• To be informed • Access • Rectification • Erasure	• Restriction of processing • Data portability • Objection • Rights in relation to automated decision making and profiling

Any person who wishes to exercise their data protection rights may do so by using a Subject Access Request Form (Appendix 3) or by contacting the DPO:

Email: dataprotection@carlowcollege.ie

Tel: 059-9153200

Address: Data Protection Officer,
Carlow College, St Patrick's,
College Street,
Carlow.

Please provide contact details that we can use to contact you easily e.g. phone number or email address as further information may be needed to respond to your request. We may need to verify your identity, and this may include asking you to provide us with a copy of recently-issued photo-identification so that we can recognise you in our CCTV footage.

You are entitled to receive your own personal data only. Third parties may be rendered unidentifiable in any recordings or images released to you. Subject to exemptions, data subjects are entitled to receive one free copy of their personal data. The College will reply to your request within one month.

Data subjects have the right to complain to the Data Protection Commission (contact details), however, we encourage data subjects to contact us in the first instance.

4.7 Access to CCTV images

Carlow College shares CCTV images where obliged or permitted by an enactment or court order. Recipients may include relevant employees; An Garda Síochána or other law enforcement agency in connection with the prevention, detection or investigation of crime; Carlow College's processors, including the CCTV system provider, security operatives, legal advisers, insurers and any person/company contracted to carry out an investigation. Controllers may be requested to provide CCTV footage to a third party to investigate a matter. In such cases, an assessment procedure will be carried out by the DPO on a case-by-case basis to determine if access can be justified in the pursuit of a legitimate interest of either the controller or another party.

4.8 Covert recording

The use of recording mechanisms, such as CCTV systems, 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 implies the involvement of An Garda Siochána or other law enforcement agencies. Covert cameras may be used by Carlow College where approved by a representative group of senior management and following completion of a DPIA in the following circumstances:

- Where informing the individual(s) concerned that recording would take place would seriously prejudice the objective of making the recording; and
- Where there is reasonable cause to suspect that illegal activity is taking place or about to take place and the recording will assist in preventing, detecting or investigating such illegal activity.

Any such covert recording 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 use covert recording will be documented and set out how the decision was arrived at and by whom.

5. Roles and Responsibilities

- The Facilities Manager and DPO monitor compliance with this Policy on a continuous basis. Any alleged contravention of this Policy may be reported to the Facilities Manager or DPO for investigation.
- The DPO is responsible for processing all access requests.
- Authorised users are responsible for the duties assigned to them in Appendix 1. Authorised users who are processors are subject to the terms and conditions of their contracts with Carlow College.
- Any employee or other authorised user who has custody of CCTV footage or stills is responsible for its security, including timely and secure disposal.
- Senior management authorises the use of covert recording.

Employees who are found to have breached this Policy may be subject to disciplinary action, up to and including dismissal.

6. Associated Documentation

- Appendix 1 – Authorised Users (Not for publication online)
- Appendix 2 – CCTV Access Log

- Appendix 3 – CCTV Subject Access Request Form

7. Referenced Policies

- *Data Protection Policy*
- *Equality Policy*
- *Freedom of Information Policy*
- *Disciplinary Policy (Staff)*
- *Learner Code of Conduct and Disciplinary Policy*

8. Monitoring and Review

This Policy will be kept under review by the DPO and Facilities Manager in respect of legislative and/or operational change and will be formally reviewed every five years.

Appendix 1: Authorised Users ***(Not for Publication Online)***

Appendix 2: CCTV Access Log

CCTV Access Log

DATE OF VIEWING	**AUTHORISED EMPLOYEE NAME**	**ACCESS REASON / DESCRIPTION OF INCIDENT**	**DATE AND TIME OF VIEWED IMAGES**	**ACTION TAKEN** E.G. ACCESS SYSTEM, PRIOR DPO APPROVAL MUSTS EXIST TO MAKE RECORDING, EXTRACT STILL IMAGES, SHOW IMAGES TO GARDAÍ ETC

Appendix 3: CCTV Subject Access Request Form

CCTV Subject Access Request Form

This form may be used by data subject to request CCTV footage.

Completion instructions:

- Please supply contact details that we can use to contact you easily in case we need to follow up on your request. We may need further information about your request or to verify your identity.
- Completed applications may be sent to dataprotection@carlowcollege.ie or Data Protection Officer, Carlow College, St. Patrick's, College Street, Carlow, A93 A003.

Name	
Address	
Tel.	
Email	
Details of request	
To help us locate relevant CCTV images, please provide as much detail as possible: date, time, location, description of incident/accident	