TITLE: ***CCTV POLICY***

Effective Date	06 February 2019	**Version**	01
Approved By	Management Board	**Date Approved**	06 February 2019
		Review Date	06 February 2022 *or as required*
Superseded or Obsolete Policy / Procedure(s)		**Owner**	
Data Protection Policy (2014-2015)		Facilities Manager and Data Protection Officer (Jointly)	

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 College operates a CCTV system both inside its buildings and in the grounds.

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, including the General Data Protection Regulation (hereafter GDPR) and national data protection legislation; 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.

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 or 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 monitors the CCTV system on behalf of Carlow College, is an example of a processor

Personal data means any information relating to an identified or identifiable natural person (data subject).

Authorised employee means any employee 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 employees, learners and members of the public visiting the College's premises.

The Policy also applies to authorised employees who have been designated certain duties in respect of the CCTV system.

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 security of persons, property and the premises;
- To improve and provide information relating to health and safety matters;
- To facilitate investigations into serious incidents under College policies;
- To facilitate investigations into serious accidents under College policies;
- Disciplinary matters involving employees and learners of Carlow College.

CCTV is not used to monitor the attendance of employees or learners.

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 and the Freedom of Information Act 2014.
- The legal basis under which Carlow College processes CCTV images are its legitimate interests under Article 6(1)(f) of the GDPR.
- CCTV cameras operate on a 24-hour basis, seven days a week.
- Cameras capture images of Carlow College's premises only.
- Cameras will not be installed in areas where persons have a reasonable expectation of privacy.
- The Facilities Manager has responsibility for maintenance of the CCTV system, in collaboration with Building Services and Netwatch. Periodic checks are carried out to ensure that cameras are functioning satisfactorily. Maintenance work is carried out in a timely manner. A maintenance log is kept by Netwatch.
- 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.
- Notices are posted at prominent locations on the College premises indicating that a CCTV system is in operation, and provide contact details for queries.
- Carlow College will conduct a Data Protection Impact Assessment where changes to its CCTV system are proposed.

4.3 Data security

- A small number of authorised employees have access to the CCTV system in order to permit them to conduct their duties (see Appendix 1). Authorised employees are to use the CCTV system to execute their designated duties only and 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.
- Authorised employees are to access the CCTV system only in relation to an identified incident/accident.
- The CCTV system is available only on the computers of authorised employees. Access is controlled by password. Authorised employees are not to share their password with any person.
- A log of access to the CCTV system, recordings made or stills taken from the CCTV system is coordinated by the Facilities Manager. The Facilities Manager and the Data Protection Officer (hereafter DPO) ordinarily have access to the access log.
- Where an authorised employee requires to access the CCTV system to view footage they are to communicate the following to the Facilities Manager via email:
    - 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 or show images to a member of An Garda Síochána

- The Facilities Manager will enter this information in an access log.
- Where authorised employees require to extract a recording or take stills from the system, they are to notify the Facilities Manager via email, who will add this information to the access log. Authorised employees may only create recordings or take stills for their own purposes. If another employee or any other person requests same, the request is to be sent to the DPO for processing.
- Where an access request is approved, the authorised employee who extracts the images from the system is to communicate the following information to the Facilities Manager, who will enter it in the access log:
    - Name of authorised employee
    - Date and time of occurrence of images recorded on the system
    - Date on which images were copied from the system
    - The location of the occurrence of the images on the system
    - The reason why the images were copied from the system
    - The name and organisation of any person to whom images were given.
- Copies of recordings or still images will be kept securely and distributed on a need to know basis only. Recordings and stills are to be destroyed in a secure manner. Security of recordings and stills is the responsibility of the employee in whose custody they are.

4.4 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;
- Employees (other than authorised employees) who require footage or stills in connection with the execution of their duties; and
- Members of An Garda Síochána.

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 his/her 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 employee) and a decision will be made on whether or not to grant access to the CCTV images to the requesting employee and 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. The discussion/decision process described here also applies to authorised employees who are considering using CCTV images in the course of a formal 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 opportunity to respond as is imperative under fair procedures.

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[1]

Any person who wishes to exercise their rights under the GDPR may do so by written application to the DPO.

The form (at Appendix 2) may be used or the same information may be provided in another written format to dataprotection@carlowcollege.ie or Data Protection Officer, Carlow College, St. Patrick's, College Street, Carlow.

Please provide your telephone or email contact details as the College may need to contact you for further information regarding your request.

The College must verify your identity. Please include a copy of recently-issued photo-identification with your application so that we can recognise you in our CCTV footage.

You are entitled to receive your own personal data only. Third parties will be rendered unidentifiable in any recordings or images released to you.

[1] These rights are explained in further detail in the College's *Data Protection Policy*, which is available on the College website, and on the website of the Data Protection Commission: www.dataprotection.ie.

Data subjects are entitled to receive one free copy of their personal data. The College will reply to your request within one month.

4.5 Provision of access to An Garda Síochána

Access to CCTV will be provided by Carlow College to An Garda Síochána for the investigation of a particular offence in accordance with guidance issued by the Data Protection Commission. Authorised employees may give An Garda Síochána visual access to the system, however, if they request footage or stills they should be directed to apply in writing to the DPO.

Where a Garda views the system the authorised employee should record the following information and communicate it to the Facilities Manager:

- Date and time of viewing by the member of An Garda Síochána;
- The name of the person viewing the images;
- The reason for the viewing, including date, time and location of footage viewed;
- The outcome, if any, of the viewing.

4.6 Disclosures

Carlow College releases CCTV images where obliged or permitted by a court order or rule of law. Recipients may include relevant employees; An Garda Síochána in connection with the prevention, detection or investigation of crime; our processors, including Netwatch, legal advisers, insurers and any person/company contracted to carry out an investigation.

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.

Employees are responsible for the duties assigned to them in other sections of this Policy.

Any employee who has custody of CCTV footage or stills is responsible for its safety and secure disposal.

Alleged contraventions of the *CCTV Policy* may be investigated under this Policy or the College's Data Protection Policy. Employees who are found to have breached these policies may be subject to disciplinary action, up to and including dismissal.

6. Associated Documentation

- Appendix 1 – Authorised Employees
- Appendix 2 – CCTV Subject Access Request Form

7. Referenced Policies

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

- *Grievance Policy (Staff)*
- *Learner Complaints and Grievances Policy*
- *Dignity and Respect Policy*
- *Equality Policy*
- *Child Protection Policy*
- *Health and Safety 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 three years.