CCTV Policy

Author:	Tom Cooney & Louise Kenny
Sponsor:	Tom Doherty
Submitted to:	SMG
Version:	1.0
Status:	Approved

1. Introduction

This Policy sets out the basic conditions of use for Closed Circuit Television (CCTV) systems by Teagasc. It describes the purpose and location of CCTV monitoring, a contact for those wishing to discuss CCTV monitoring and guidelines for its use.

All persons involved in the planning, supervision or operation of such a CCTV scheme will familiarise themselves with this document from the outset.

This Policy document seeks compliance 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). This Policy highlights certain legal obligations set down in the Data Protection Acts and EU Regulations. In order for this Policy to remain relevant to the day to day activities of CCTV operation, it needs to be updated as practice and understanding of the laws in this area develop. Accordingly, this Policy will be kept under review to ensure that it remains relevant in the context of changes in technology, and compliant with any developments in this area.

2. Purpose of Policy

The purpose of this policy is to ensure that Teagasc's use of CCTV complies with relevant legislation, regulations and standards - the Data Protection Acts 1988/2003/2018 and Regulation (EU) 2016/679 (GDPR).

3. Purpose of CCTV System

CCTV surveillance at Teagasc is intended for the purposes of:

- Overt Monitoring; Surveillance is performed using devices that are visible and obvious and which are notified by easily-read and well-lit signs in prominent positions. The locations of all cameras are listed in the Teagasc CCTV Schedule.
- Deterring, detecting and defending against criminal, malicious and anti-social behaviour on property and persons on Teagasc sites;
- Protecting Teagasc buildings and assets;
- Promoting the safety and security of staff, contractors, students and guests by helping to secure a safer environment;
- Investigating accidents or dangerous occurrences;
- Supporting an Garda Síochána in deterring and detecting crime;
- Assisting in identifying, apprehending and prosecuting offenders;
- Identifying the occurrence of anti-social activity that may give rise to disciplinary proceedings;
- Scientific Research Purposes.

4. Scope

This applies to all personnel utilising Teagasc premises including, but not limited to Teagasc staff, students, employees, contractors, visitors and members of the general public.
This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material by Teagasc and third parties. Teagasc will ensure that CCTV systems, where installed, are operated only in a way that is compatible with the provisions of this policy.

5. General Principles

Teagasc has a statutory responsibility to protect Teagasc property and equipment as well as providing a sense of security to its staff, students and invitees to its premises.

Teagasc owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and its associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life at Teagasc premises by integrating the best practices governing the surveillance of its premises.

The primary aim of the CCTV monitoring of Teagasc premises is to deter, detect and defend against crime and vandalism and to assist in the protection and safety of the said property and its associated equipment and materials.

CCTV monitoring of public areas, for security purposes, will be conducted in a manner consistent with this policy.

Monitoring for security purposes and all purposes outlined in Section 3 above will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies and personnel for any other purpose is prohibited by this policy. For example CCTV monitoring of political or religious activities, or employee evaluations would undermine the acceptability of the resources for use regarding critical safety and security objectives and is therefore prohibited by this policy.

Video monitoring of public areas, for security purposes, within each campus/Teagasc building, is limited to areas that do not violate the reasonable expectation to privacy as defined by law. Attention is drawn to the Teagasc Data Protection Policies at http://dms/DP/Pages/Data%20Protection%20Policies.aspx. Reasonable expectation of privacy means that any limitation of the person's right to privacy should be proportionate to the likely damage to Teagasc's legitimate interests if such monitoring did not take place

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by Teagasc. Recognisable images captured by CCTV systems are "personal data." They are therefore subject to the provisions of the

Data Protection Acts 1988, 2003 and 2018 and the General Data Protection Regulation (EU) 2016/679 ("GDPR")

No CCTV systems or recording systems of any description may be installed or used on Teagasc property without the express written permission of the Head of Corporate Services & Procurement and the Data Protection Officer.

6. JUSTIFICATION FOR USE of CCTV

The use of CCTV to monitor Teagasc premises for security purposes has been deemed to be justified by Teagasc where it is satisfied that there is a proven risk to security and safety of Teagasc personnel, contractors, visitors, staff and the general public, as well as Teagasc assets, when no CCTV is present and that the installation of CCTV is proportionate in addressing such issues.

The system's purpose is to deter unauthorised entry, to detect unauthorised entry and malicious behaviour, and to assist in the defence of Teagasc property & personnel.

7. ACCESS

In relevant circumstances, CCTV footage may be accessed:

- By authorised Teagasc Personnel (see below);
- By An Garda Síochána where Teagasc are required by law to make a report regarding the commission of a suspected crime;
- By third party security companies retained by Teagasc to operate CCTV and other security functions;
- Following a request, by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Teagasc property;
- By third party providers who provide security services to Teagasc;
- By data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to Teagasc (see Teagasc's Data Subject Request Policy);
- By individuals (or their legal representatives) subject to a court order;
- By Teagasc's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property or persons;

- Where there has been a suspected or actual breach of the Teagasc Dignity at Work policy;

- By State bodies or agencies that have a legal entitlement to access this data.

Information obtained through video monitoring may be downloaded from the system and viewed by campus administrative staff only when authorised by The Director, a Head of Directorate, the Data Protection Officer or the following Site Managers, and any staff member delegated to act in the place of the Site Managers, but only for their area of responsibility, as appropriate:

Authorised Officer	Scope of Authority
College principal and his/her superiors	The College for which he/she is responsible.
Advisory Regional Manager and his/her superiors	Advisory Offices in the Region for which he/she is responsible.
Enterprise leader and Moorepark campus manager and his/her superiors	The campus and associated farms for which he/she is responsible or is the manager.
Head of Corporate Services and Procurement and his/her superiors	Head Office and associated buildings.

Information obtained through video monitoring may also be downloaded from the system and viewed by those parties listed in Section 7

The Site Manager will have responsibility for ensuring the proper and efficient and orderly day to day operation of the CCTV system, for making staff aware of who is responsible for responding to data requests and the day to day operation of the CCTV on each site including access to the CCTV system (see section 11). The Manager may delegate these responsibilities as the Manager deems appropriate.

In line with best practice and the requirements of the Teagasc Data Subject Request Policy, Teagasc has formalised its approach to handling requests from Data Subjects to exercise their rights in relation to their Personal Data under its control.

Any person whose image is recorded on a CCTV system has a right to seek and be supplied with a copy of their own personal data from the footage. To exercise that right, a person is asked to make an application in writing (Appendix 2- "Subject Access Request" format).

Such requests shall be made to Teagasc and shall provide Teagasc with a reasonable indication of the timeframe of the recording being sought i.e. they will provide details of the approximate time and the specific date(s) on which their image was recorded (see Appendix 2 - Data Access Request for the suggested format for any requests.).
Requests should be sent by email to dpo@teagasc.ie or by post to:

The Data Protection Officer, Teagasc Head Office, Oak Park, Carlow.

If Teagasc receives a request where it is not the Data Controller, the request will be returned to the requestor and Teagasc will notify the requestor of the identity of the Data Controller should it have that information and it be lawful to supply it.

Where there are images of other staff/personnel present in the data requested, these may need to be pixelated and redacted.

If a law enforcement authority, such as An Garda Síochána, is seeking a recording for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request made by An Garda Síochána will be requested in writing and Teagasc may seek legal advice.

If CCTV footage which is the subject of a criminal investigation by an Garda Síochána is requested by a data subject by means of a data subject access request, access may be refused under Data Protection Act legislation.

8. LOCATION OF CAMERAS

The location of cameras is a key consideration. Cameras will be sited in such a way that they only monitor those spaces which are intended to be covered by the system.

Teagasc, on the advice of the CCTV Contractor, endeavours to select locations for the installation of CCTV cameras which are least intrusive and which protect the privacy of individuals. Teagasc will only use the cameras in order to achieve the purposes for which the system has been installed.

Cameras will be in positions to allow the recording of external and internal areas and placed in such a way as to prevent or minimise the recording of passers-by, or of another person's private property.

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.

A risk assessment will be used in each location to identify valuable movable assets. This assessment will also determine what quality of camera is needed in each area. The following areas will be considered:

- Research crops that could be subject to vandalism
- Livestock which could be subject to theft.
- There may be reasonable need to examine perimeter fencing around farm buildings.

A Data Protection Impact Assessment will be carried out at each location to identify CCTV impact on the rights and freedoms of natural persons.

9. NOTIFICATION – SIGNAGE

Teagasc will provide a copy of this CCTV Policy on request to staff, students and visitors to Teagasc premises. It will also be accessible via the Corporate Services section of the Tnet and the Teagasc public website.

Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation.

Adequate signage will also be prominently displayed at the entrance to Teagasc property where there is CCTV in operation.

Signage shall include the name and contact details of Teagasc as well as the specific purpose(s) for which the CCTV camera is in place in each location.

WARNING
CCTV cameras in operation
Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, for the safety of our staff, students, guests and for the protection of Teagasc and its property.
This system will be in operation 24 hours a day, every day.
These images may be passed to An Garda Síochána [include any other third parties who may have access to CCTV footage including any security firms engaged by Teagasc]
This scheme is controlled by Teagasc [and operated by <insert name of commercial security company where one is used if none is used insert "Teagasc"]
For more information contact ……*<local phone number>*……

Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, gates
- reception area
- at or close to each internal camera (if any)

10. STORAGE & RETENTION

CCTV images will be retained for no longer than is necessary.

The images captured by the CCTV will be retained for a maximum of one year, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue or is required for scientific purposes.

The recorded footage and the monitoring equipment shall be securely stored with a log of access kept by the Site Manager. Unauthorised access to that storage facility is not permitted at any time. The storage facility is locked when not occupied.

11. RESPONSIBILITIES

Site Managers will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Teagasc.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within Teagasc.
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.
- Ensure that the CCTV monitoring at Teagasc is consistent with the highest standards and protections.
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- Maintain a record of access (e.g. an access log) to or the release of tapes / storage media or any material recorded or stored in the system.
- Maintain a record of the number and nature of enquiries received together with an outline of each action taken.
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.
- Give consideration to staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
- Ensure through the implementation of a Data Protection Impact Assessment that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within Teagasc and be mindful that no such infringement is likely to take place.
- Ensure that cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of “Reasonable Expectation of Privacy”.
- Ensure that images/recordings are stored for a period not longer than set out in section 10.
- Ensure that camera control is solely in compliance with this policy.
- Ensure that camera control is not infringing an individual’s reasonable expectation of privacy in public areas.

12. SECURITY COMPANIES

Where a CCTV system is controlled by a security company, contracted by Teagasc the following applies:

- Cameras must be installed and controlled by contractors certified by The Private Security Authority.

- Teagasc will implement a written contract with the security company. This contract will detail the areas to be monitored, how long data is to be stored, what the security company may do with the data, what security standards will be in place and what verification procedures apply. The written contract also states that the security company will give Teagasc all reasonable assistance to deal with any subject access request made under Article 15 of the GDPR which may be received by Teagasc within the statutory time-frame (one month).

- There must be a records folder (electronic) in place to record all documents relating to:
  - Installing the CCTV, including but not limited to: site surveys including that of informal access points,
  - Review plan
  - Maintenance plan and records
  - Certificates from installer/contractor
  - Test results from test data request showing other faces obscured.

- Cameras will be properly maintained and serviced to ensure that clear images are recorded.

- The Data Processor operates under the instruction of Teagasc. Article 28 GDPR places a number of obligations on data processors. These include having appropriate 'technical and organisational' measures in place to protect personal data and to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network and against all unlawful forms of processing. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted.

- All security company staff will be made aware of their obligations relating to the security of data.

- Cameras will, as far as possible, be protected from vandalism in order to ensure that they remain in working order.

- If a camera is damaged, there will be clear procedures for:
  - Ensuring that the camera is repaired within a specific time period.
  - Monitoring the quality of the maintenance work.

13. Appeals process

Where a person to whom this policy applies has a concern in relation to the policy itself, or its implementation, that person should contact the Data Protection Officer outlining their concerns.

Any person also has a right to raise concerns with the office of the Data Commissioner and contact details may be found here:
https://www.dataprotection.ie/en/contact/how-contact-us

14. IMPLEMENTATION & REVIEW

The policy will be reviewed and evaluated from time to time. On-going review and evaluation will take cognisance of changing information or guidelines e.g. from the Data Protection Commissioner, An Garda Síochána, Audit units (internal and external to Teagasc), the Article 29 Working Party (The European Data Protection Board) and the European Commission, national management bodies, legislation and feedback from staff and others.

The date from which the policy will apply is the date of adoption by Teagasc. Implementation of the policy will be monitored by the Site Managers.

15. Enforcement

Breaches of this policy may result in HR disciplinary procedures as set out in the Staff Handbook being invoked. Individuals should be aware that they as well as the organisation are individually liable to summary conviction under the Data Protection Acts if found guilty of knowingly or recklessly contravening its provisions. Breaches by individuals who are not staff will be dealt with in accordance with the law

16. Related Documents

- Teagasc Data Protection Policy
- Teagasc Data Breach Management Policy
- Teagasc Data Subject Request Policy
  The above documents may be found at
  http://dms/DP/Pages/Data%20Protection%20Policies.aspx

- EU General Data Protection Regulation ("GDPR")
- Data Protection Act 1988
- Data Protection (amendment) Act 2003
- Data Protection Act 2018

17. APPENDIX 1 – DEFINITIONS

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

CCTV	Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.
The Data Protection Acts	The Data Protection Acts 1988, 2003 and 2018 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All Teagasc staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation.
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[1]
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.
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

[1] Regulation (Eu) 2016/679 Of The European Parliament And Of The Council, Article 4(1)

Data Subject	an identified or identifiable natural person
Data Controller	Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In this case it will be Teagasc.
Data Processor	Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors”,

APPENDIX 2 - SUBJECT ACCESS REQUEST FORM

Date issued: _____

Access Request Form: Request for a copy of Personal Data under the GDPR and the Data Protection Act 2018

Full Name	
Address	
Contact number *	Email addresses *

** We ask for this as we may need to contact you to discuss your access request*

I, ……..[insert name] wish to be informed whether or not Teagasc holds personal data about me and to be provided with a description of this data and to be informed of the purpose for holding such data. I am making this access request under **Article 15(1) of the General Data Protection Regulation**.

☐

AND/OR

I, …….. [Insert name], wish to make an access request for a **copy** of any personal data that Teagasc holds about me. I am making this access request under **Article 15(3) of the General Data Protection Regulation**.

☐

Any other information relevant to your access request (e.g. if requesting images/recordings made by CCTV, please state the date, time and location of the images/recordings (otherwise it may be very difficult or impossible for Teagasc to locate the data).

Signed …… Date ……

Checklist: Have you:

1) Completed the Access Request Form in full? ☐

2) Signed and dated the Access Request Form? ☐
3) Included a photocopy of official/State photographic identity document (driver's licence, passport etc.) *****. ☐

***Note to Teagasc**: Teagasc will satisfy itself as to the identity of the individual and make a note in the records that identity has been provided, will not retain a copy of the identity document.