

Comhairle Contae Mhuineacháin

Monaghan County Council



Community CCTV Policy

Adopted by Management Team at its meeting on

9th February 2021

CONTENTS

INTRODUCTION

- 1.0 Policy Statement
- 2.0 Policy Purpose
- 3.0 Policy Scope
- 4.0 Legislation
- 5.0 Purpose of Community CCTV
- 6.0 Roles and Responsibilities
- 7.0 Security Companies/data Processors
- 8.0 Summary Description and Technical Specifications for the CCTV System
- 9.0 Siting of Cameras
- 10.0 Quality of the Images from CCTV
- 11.0 Security and Controls
- 12.0 Notifications, Information and Signage
- 13.0 Access to the Images
- 14.0 Data Subject Rights and Access Requests
- 15.0 Access requests from An Garda Siochana
- 16.0 Access requests in relation to data processed for law enforcement purposes
- 17.0 Data Breach
- 18.0 Retaining Information
- 19.0 Installation of a New Community CCTV Scheme or Upgrade of an Existing Scheme
- 20.0 Community CCTV systems and risk assessment
- 21.0 Approval of Community CCTV Systems
- 22.0 Data Protection
- 23.0 Policy Review
- 24.0 Definitions

Monaghan County Council Community CCTV

INTRODUCTION

1.0 Policy Statement

- 1.1 CCTV and surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for the members of our Community. This role must be balanced, proportionate and undertaken in compliance with data protection law. This policy is intended to assist staff and others in complying with legal obligations when working with personal data using Community CCTV within County Monaghan.
- 1.2 Any questions in relation to this policy should be directed to Monaghan County Council's DPO at dataprotectionofficer@monaghancoco.ie
- 1.3 Monaghan County Council has Community CCTV systems in place in a number of locations throughout the County for the sole and primary purpose of securing public order and safety in public places.
- 1.4 Images are monitored and recorded at each location and will be used in strict accordance with this policy. These systems are owned by Monaghan County Council and Community Groups.
- 1.5 Community CCTV systems operated by Monaghan County Council are regulated in accordance with the Data Protection Acts 1988-2018 (as amended), the General Data Protection Regulation (**GDPR**) and the Garda Síochána Act 2005 (the '**Acts**').
- 1.6 For the purpose of the Acts, the Data Controller is Monaghan County Council.
- 1.7 Where images captured by surveillance technology are capable of identifying a natural person, they constitute personal data and are covered by the Acts. This Policy is associated with Monaghan County Council's Privacy Notices and Data Protection Policies, the provisions of which should be adhered to at all times.
- 1.8 Our data protection contact for the purpose of the Acts is:

Data Protection Officer:

Pauline McClean

Email: dataprotectionofficer@monaghancoco.ie

Security Officer:

Suzanne Monahan

Email: smonahan@monaghancoco.ie

2.0 Policy Purpose

- 2.1 The purpose of this policy is to outline the procedures and safeguards in place regarding the operation of and access to the CCTV systems, and the resultant images.

3.0 Policy Scope

- 3.1 This policy applies to all Monaghan County Council staff, interns and temporary workers, An Garda Siochana, Security Companies, Consultants, Contractors and to all Community CCTV systems operated by Monaghan County Council.

4.0 Legislation

- 4.1 The lawful bases for the processing of Community CCTV are: -
- 4.2 General Data Protection Regulation (GDPR) and the Data Protection Act 1988-2018 (as amended and
- 4.3 The Garda Siochana Act 2005
- 4.4 The following Data Protection Principles apply to the use of CCTV. Personal data must be:
- Processed lawfully, fairly and in a transparent way ('transparency');
 - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (except for archiving in the public interest) ('purpose limitation');
 - Adequate, relevant and limited to what is necessary for the purposes its being processed ('data minimisation');
 - Accurate and kept up to date ('accuracy');
 - Kept safe and secure using appropriate technical and organisational measures ('integrity and confidentiality');
 - Retained for no longer than is necessary for the specified purpose ('storage limitation').

Monaghan County Council must be able to demonstrate compliance with each of these principles ('accountability').

The law requires that any proposed Community CCTV scheme must:

- be approved by the local Joint Policing Committee;
- have the prior support of the relevant local authority, which must act as data controller;
- and have the authorization of the Garda Commissioner.

5.0 Purpose of Community CCTV

Community CCTV systems have been installed by Monaghan County Council in conjunction with An Garda Síochána in accordance with Section 38 of the Garda Síochána Act 2005 where Monaghan County Council is the Data Controller. The purpose of Community CCTV is to secure public order and safety and to deter illegal or anti-social behaviour in public places. This purpose will be achieved by monitoring the systems to:

- Deter those having criminal intent;
- Assist in the prevention and detection of crime and to investigate security incidents to secure evidence, should such incidents occur;
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order.

Monaghan County Council has installed Community CCTV at the following locations: -

- Mullaghmat – installed by Mullaghmat/Cortolvin Community Development Association;
- Castleblayney Town;
- Playgrounds and public car parks

6.0 Roles and Responsibilities

- 6.1 Authorisation for the installation of Community CCTV is granted under Section 38 of An Garda Síochána Act 2005. The Community CCTV systems in use, shall be managed by external security companies on behalf of Monaghan County Council. They shall be responsible for the installation, maintenance and day to day operation of the systems.
- 6.2 Monaghan Joint Policing Committee shall establish a separate Community CCTV Steering Group as a sub-committee to the JPC to oversee the management of the Councils Community CCTV systems. The Group shall consider the installation of new or upgrade of Community CCTV schemes, recommend locations of cameras, identify issues, consider complaints and monitor the effectiveness of Community CCTV systems. Details of Terms of Reference are contained in **Appendix 1**.
- 6.3 Each Community CCTV system is accessed as necessary by authorised staff of Monaghan County Council and designated staff of external security companies acting on behalf of Monaghan County Council. Images captured by each system are

monitored and recorded in individual control rooms. Monitors are not visible from outside the control room.

- 6.4 No unauthorised access to the individual control rooms will be permitted at any time. Access will be strictly limited to authorised staff, authorised members of the Community, designated staff of external security companies, authorised members of senior management, An Garda Síochána and any other person with statutory powers of entry.
- 6.5 Staff and visitors may be granted access to the individual control room on a case-by-case basis and only then on written authorisation from the relevant Head of Section. 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 individual control rooms. All visitors will be required to complete and sign the visitor's log book.
- 6.6 Following consultation with the Data Protection Officer, the Director of Services and each Head of Section has overall responsibility for overseeing the management of Community CCTV within their respective directorate, and ensuring the designated staff are adequately trained and informed of the appropriate use of CCTV.
- 6.7 The Data Protection Officer is responsible for monitoring compliance with this policy.

7.0 Security Companies/Data Processors

- 7.1 All Community CCTV systems shall be controlled, maintained and managed by external security companies contracted by Monaghan County Council. The following shall apply:
 - Security companies that place and operate Community CCTV systems on behalf of Monaghan County Council are considered to be 'Data Processors'. As Data Processors, they must only act on the instructions of the Data Controller (i.e., Monaghan County Council). Articles 28-32 of the GDPR sets down a number of obligations in respect of Data Processors. These include having appropriate security measures in place to prevent unauthorised and unlawful access to and alteration, disclosure or destruction of the personal data. At a minimum robust encryption should be in place where remote access to live recording is permitted.
 - Monaghan County Council shall only engage a processor to act on its behalf where:

- a. The Security Company is licenced with the Private Security Authority (PSA) which is a statutory body with responsibility for licensing and regulating the private security industry in Ireland;
 - b. There is a **written agreement** in place between the two parties which contains the provisions required by Article 28 of the GDPR **and**
 - c. The Processor provides sufficient guarantees and assurances that it will implement the appropriate **technical and organisational measures** required to comply with GDPR and to protect the rights and freedoms of data subjects.
- The appropriate contractual documentation should be obtained from the DPO in all instances.
 - An appropriate level of due diligence from a data protection perspective should be carried out in respect of any Data Processor before their CCTV/security services are engaged.
 - Staff of the security company must be made aware of their obligations relating to the security of data.

8.0 Summary Description and Technical Specifications for the CCTV systems (*This Section shall be reviewed and amended where necessary by IT and Security Companies acting on behalf of the Council*)

- 8.1 The CCTV systems are conventional static systems. They record digital images and are equipped with motion detection. They record any movement detected by the cameras in the area under surveillance, together with time, date and location.
- 8.2 All cameras operate 24 hours a day, seven days a week.
- 8.3 The image quality in most cases allows identification of those individuals in the camera's area of coverage.
- 8.4 Most cameras are fixed or may facilitate a swivel action.
- 8.5 Monaghan County Council shall retain a record of all Community CCTV cameras within their control and the locations of each camera in a separate Community CCTV Register.

9.0 Siting of Cameras

- 9.1 It is essential that CCTV equipment is sited in such a way that it only monitors those areas intended to be covered by the equipment.

10.0 Quality of the Images from CCTV

- 10.1 It is important that the images produced by the equipment are as clear as possible in order to ensure that they are effective for the purposes for which they are intended.
- 10.2 The equipment and recording media should be maintained on a regular basis and upgraded if necessary, to ensure the quality of the images is upheld.
- 10.3 Although every effort has been made to ensure maximum effectiveness of the CCTV systems, it is not possible to guarantee that the systems will detect every incident taking place within the area of coverage.

11.0 Security and Controls *(to be reviewed by IT Staff and Security Company)*

- 11.1 In order to protect the security of the CCTV system, a number of technical and organisational measures have been put in place, including:
- Access rights to users are granted only to those where it is strictly necessary for them to carry out their work;
 - Only the Director of Services or his/her Deputy (after consulting with Monaghan County Council's Data Protection Officer) can grant, alter, or annul any access rights of any persons;
 - Once a hard drive has reached the end of its use it will be erased prior to secure disposal;
 - All CCTV systems are password protected.
- 11.2 Security Companies are responsible for carrying out maintenance on a regular basis. Monaghan County Council shall maintain a CCTV maintenance log containing details of all regular checks and maintenance carried out.

12.0 Notifications, Information and signage

- 12.1 Data subjects must be notified of and provided with certain information in relation to this processing activity being carried out by Monaghan County Council. This information is included in appropriate signage and in Monaghan County Council's Privacy Notice.
- 12.2 It is also essential that signage is displayed in a prominent place where it will be clearly seen by members of the public. Signage will be displayed on approach routes entering the CCTV areas and in or close to the CCTV camera locations. Signage shall include:
- The identity and contact details of the Data Controller
 - The purposes for which the CCTV is in place
 - The legal basis for the processing
 - The retention period for the CCTV footage

13.0 Access to the images

- 13.1 It is important that access to, and disclosure of images and recordings are strictly controlled and documented. This is to ensure that the rights of the individual are maintained, and that the chain of evidence remains intact should the images be required for evidential purposes.
- 13.2 All access to images and recordings will be recorded in the Community CCTV **Access Log** detailing the time, date, name of authorised person and reason for accessing the system.
- 13.3 Access to CCTV images is strictly limited to the members of Monaghan County Council staff where it is necessary for them to carry out their work and/or security companies acting on its behalf.
- 13.4 All authorised staff requiring access to the CCTV images shall undergo Garda vetting by Monaghan County Council.
- 13.5 For the purpose of electronic audit trail, all authorised staff including designated staff of external security companies shall be provided with a unique identifier to access the images.
- 13.6 The granting of access permissions shall be determined and approved by the relevant Director of Services.
- 13.7 Access to images by third parties:

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

Access to these images will normally be through the following: Request from law enforcement agencies by Court Order, Freedom of Information access request or a Data Subject Access Request.

14.0 Data Subject Rights and Access Requests

- 14.1 CCTV images of an identifiable natural person are personal data and are covered by the Acts. Anyone who believes that they have been filmed by CCTV or other surveillance technologies is entitled to ask for a copy of the data from the Data Controller (Monaghan County Council), subject to exemptions contained in the Acts. They do not have the right of instant access.
- 14.2 Monaghan County Council has a Data Subject Access Request Protocol in place which should be referred to when a request is received.
- 14.3 A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Officer at County Offices, The Glen, Monaghan, H18 YT50 or by email to dataprotectionofficer@monaghancoco.ie.
- 14.4 The Data Protection Officer will then arrange for a copy of the data to be compiled and given to the data subject. All communications with the data subject must go through the Data Protection Officer. A response will be provided promptly and in any event within one month of the request having been made, subject to receiving satisfactory proof of identification from the data subject.

- 14.5 The Acts provide the right to refuse a request for a copy of the data in certain circumstances, particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. The application of this right of refusal will be managed by the Data Protection Officer.
- 14.6 If it is decided that a data subject access request is to be refused, the reasons will be fully documented, and the data subject informed in writing, stating the reasons.
- 14.7 A third party's personal data (i.e. data relating to an individual who is not the person making the request) should never be released in response to a Data Subject Access Request. Individuals who are not the data subject should be disguised from the footage/images before release, through pixilation, redaction etc. If it is not possible to disguise the images, an external company may be contracted to facilitate this.
- 14.8 Requests cannot be complied with where there are insufficient details supplied relating to the date and time of recording. Correspondence is to be sent to the requester advising them of this.
- 14.9 If the data subject wishes to view the images on site, as opposed to a copy being sent, the viewing should take place in a closed office with only the relevant individuals present.
- 14.10 If a data subject is not satisfied with the outcome of a data subject access request from Monaghan County Council, the data subject is entitled to make a complaint to the Data Protection Commission who may investigate the matter further.

The Data Protection Commission's website is www.dataprotection.ie.

15.0 Access requests from An Garda Síochána

- 15.1 In line with Sections 41 and 71 of the Data Protection Act 2018 and guidance from the Data Protection Commission, Monaghan County Council may disclose personal data to An Garda Síochána where **necessary** and **proportionate** in relation to the following purposes:
- For the prevention, detection, investigation and prosecution of crime
 - In order to prevent a threat to national security, defence or public security
 - When it is required urgently to prevent injury or other damage to the health of a person, or serious loss of or damage to property
 - When it is required by, or under any enactment, or by a rule of law or order of a Court.

- 15.2 Requests must be made on the official Garda Data Protection Form, quoting the Pulse Incident number, details of the request and signed by the Superintendent in charge.
- 15.3 In extreme emergency situations, requests in writing may be submitted after the fact.
- 15.4 If An Garda Síochána wishes to simply view the footage on the premises, this does not raise any specific data protection concerns.

16.0 Access requests in relation to data processed for law enforcement purposes

16.1 Subject to certain exemptions, data subjects have the following rights in respect of CCTV used for law enforcement purposes:

- Information rights (i.e., privacy notices and signage indicating that CCTV is in use)
- The right of access, through Data Subject Access Requests
- The right to rectification or erasure
- The right to restrict processing and
- The right not to be subject to automated decision-making

Data subjects do not have the right to object or the right to data portability in respect of processing for law enforcement purposes.

16.2 Under **Section 94 of the Data Protection Act 2018**, the above rights are restricted, and Monaghan County Council may refuse to comply with a request to the extent that is necessary and proportionate in order to;

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others

17.0 Data Breach

17.1 In the event of a data breach concerning personal data collected from Monaghan County Council's Community CCTV, the Council's Data Protection Officer must be notified immediately and provided with all the details necessary to assess whether there is a high risk to the rights and freedoms of the individuals.

17.2 Monaghan County Council are responsible for reporting data breaches to the Data

Protection Commission within 72 hours of becoming aware of the breach.

18.0 Retaining Information

- 18.1 It is important that the images are not retained for longer than is considered necessary for the purposes for which they are processed. Therefore, unless the images are required to investigate an incident, they will not be retained beyond a maximum of twenty-eight days. After **28 days** the footage will be automatically overwritten.

19.0 Installation of a New Community CCTV Scheme or Upgrade of an Existing Scheme

- 19.1 In order for the Council to install a new or upgrade existing CCTV schemes, including deploying additional cameras, funding shall first be identified;
- 19.2 Applications shall be considered by the Community CCTV Steering Group based on clear objectives and valid reasons for the requirement of the CCTV or camera(s) at the locations identified;
- 19.3 An Garda Síochána shall provide any information that could assist in the justification of CCTV at the proposed location(s).

20.0 Community CCTV systems and risk assessment

- 20.1 Following consultation with the Data Protection Officer, before any new Community CCTV system is implemented, the relevant Section of Monaghan County Council must:
1. Carry out a risk assessment in respect of the processing which evaluates the risks to the rights and freedoms of individuals arising from the processing;
 2. Carry out a **Data Protection Impact Assessment** in respect of the processing (as required by Article 35 of the GDPR and Section 84 of the Data Protection Act 2018)
 3. Implement the security measures set out in Section 77 of the Data Protection Act 2018.

21.0 Approval of Community CCTV Systems

- 21.1 The preliminary plans for the new/upgrade CCTV Scheme shall be referred to the Community CCTV Steering Group for consideration. If the proposed scheme is

deemed necessary, it shall be referred to the Monaghan Joint Policing Committee for support and initial approval;

- 21.2 A public consultation shall take place for a period of six weeks inviting submissions;
- 21.3 The consultation shall be advertised in the local paper and the Council's website;
- 21.4 The public consultation report shall be considered by the Community CCTV Steering Group and approved by Monaghan Joint Policing Committee;
- 21.5 The Joint Policing Committee shall consider the request for the new/upgrade CCTV Scheme and if in agreement;
- 21.6 A detailed design of the system and a Data Protection Impact Assessment shall be completed. The Application form for authorisation to operate a CCTV system under Section 38 (3)(c) of the Garda Siochana Act shall be submitted to the District Superintendent.
- 21.7 The Chief Superintendent shall decide if it is appropriate for the application to be forwarded to the CCTV National Advisory Committee for authorisation by the Garda Commissioner of the new proposed CCTV scheme or the upgrade/extension of the existing scheme under Section 38 (c) of the Garda Siochana Act 2005 for the sole and primary purpose of securing public order and safety in public places.

22.0 Data Protection

- 22.1 Monaghan County Council is committed to the protection of personal data and respects the fundamental rights and freedoms of individuals. It collects and processes a significant amount of personal data and Special Category personal data in various multiple formats.
- 22.2 For the purpose of the Data Protection Acts 1988 – 2018 (as amended) and the General Data Protection Regulation (GDPR) the Council processes personal data in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access to and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

23.0 Policy Review

- 23.1 This policy will be reviewed and evaluated yearly. Ongoing review and evaluation will take cognisance of changing information or guidelines, legislation and feedback from staff and others.

24.0 Definitions: -

- 24.1 **Personal Data:** - means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- 24.2 **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;
- 24.3 **Processor:** - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- 24.4 **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;
- 24.5 **Data Subject:** - is a natural living person who is the subject of personal data;
- 24.6 **DPO:** - Data Protection Officer;
- 24.7 **CCTV:** - Closed Circuit Television.