Comhairle Contae
Fhine Gall
Fingal County
Council

# Fingal County Council
# CCTV Policy

## Introduction

Closed Circuit Television Systems (CCTV) are installed in the offices, properties, plant, civic amenity and other locations in the ownership of Fingal County Council, County Hall, Main Street, Swords and may also be used by staff when working alone.

The Council undertakes to operate its CCTV and undertakes to ensure that those who operate CCTV on its behalf do so within the terms of this policy and the law and will review it regularly to ensure continuing compliance with the Data Protection and Freedom of Information Acts and Section 38 of the Garda Síochána Act, 2005.

## 1. Personal Data

CCTV capture data, i.e., images of persons, which is their personal data. This confers rights on them under the Data Protection Acts. Importantly, the Council has duties and obligations as the holder of personal data, as in these cases, and must ensure such data is handled and managed correctly.

This policy document addresses these issues and sets out clearly what Fingal County Council, as Data Controller, must do to protect personal data in relation to CCTV.

## 2. Private and Public CCTV Systems

The Council operates two types of CCTV Systems, private systems and public systems.

***Private systems*** operate at Council premises such as offices and other locations where the public do not have a right of access, be it implied or express. While there may be some capture of persons passing by the front of such buildings these CCTV are considered to be private and do not need consent of the Garda Commissioner.

***Public systems*** operate in public places such as on streets, on roadways, bridges, at Bring Centres and other public places where the public have either an implied or express right of access. Public places may also include locations within Council offices such as main corridors which the public has access to as well as library buildings open to the public.

This policy distinguishes between private and public CCTV by noting that normally,

for public CCTV, the consent of the Garda Commissioner is needed under Section 38 of the Garda Síochána Act, 2005.

The Council may also use personal recording CCTV worn on staff in the course of their duties. This is for Health & Safety reasons and for purposes affecting their work in public.

Whether CCTV are located in a private or public location, or worn by staff, this policy applies to these systems equally as do all the controls and standards as set out below.

## 3. Video and Audio Recordings

CCTV in this policy document includes both video recording and audio recording systems.

## 4. Purpose of Policy

The purpose of this policy is to regulate the use of Closed Circuit Television Systems and its associated technology in the monitoring of:

*A: Internal and external environs of premises under the remit of Fingal County Council*
*B: The ongoing security of staff working alone or in handling law enforcement matters*
*C: Public areas*
*D: The occasional use of CCTV for covert purposes such as monitoring litter black spots*
*E: Such other purposes as may arise from time to time*

CCTV is installed to enhance the security of our premises as well as to create a mindfulness among occupants and visitors that a surveillance security system is in operation at all times. Specifically, such CCTV surveillance is intended for the purposes of:

- protecting the Council's buildings and assets, both during and after office hours

- promoting the health and safety of staff, visitors and customers
- prevention of bullying
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism)
- supporting the Garda in a bid to deter and detect crime and
- assisting in identifying, apprehending and prosecuting offenders, and
- in respect of the usage by staff of CCTVS to ensure persons interacting with staff are aware that their actions are being recorded

**5. Scope**

This policy relates to the locating and use of CCTVs, their monitoring, recording, security, control and use of recorded material as well as setting out the way by which persons and others can seek to see images and to ensure that CCTVS are operated in a manner compatible with this policy.

**6. General Principles**

Fingal County Council is responsible for the protection of its property, equipment and other plant as well as for staff, elected members, visitors and customers to its premises. Usage of CCTV contributes to compliance with the Safety, Health and Welfare at Work Act, 2005.

In terms of public CCTV while the Council has a limited role in law enforcement in relation to its specific functions, CCTV may be provided in public places to facilitate the deterrence, prevention, detection and prosecution of offences as well as enhancing public safety and security.

The use of CCTV will be conducted in a professional, ethical and legal manner within the terms of this policy and the law and all CCTV and associated equipment are required to be compliant with this policy.

Data obtained by CCTV may only be released when authorised by the Data Protection Officer or others as designated. Requests for CCTV recordings / images / sounds from An Garda Síochána or other law enforcement agencies will be facilitated subject to proper audit trail and within the law.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the Council, including Equality & Diversity Policy, Dignity at Work Policy, Codes of Practice for dealing with

complaints of Bullying & Harassment and Sexual Harassment and other relevant policies and guidelines such as those issued by the Office of the Data Commissioner.

Video monitoring of public areas and within the Council's offices & premises for security purposes is limited to uses that do not violate the individual's reasonable expectation to privacy. CCTV will not be located in areas where staff and the public would expect absolute privacy. Privacy Impact Assessment will be undertaken where necessary.

Recognisable images captured by CCTV systems are "personal data" and subject to the provisions of the all current Data Protection legislation including, EU GDPR and Data Protection Act 2018.

## 7. Justification for Use of CCTV

Article 5, Section 1 (c) of the EU GDPR 2016/679 requires that data is "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed* ".
This means that the Council must be able to justify the obtaining and use of personal data by means of a CCTV system. The following uses are considered to be justified -

- The use of CCTVS to control the perimeter of Council buildings and property for security purposes is deemed to be justified and can be used to capture images of intruders or of individuals damaging property or removing goods without authorisation.
- In other areas of offices where CCTV has been installed, e.g. hallways, stairwells, locker areas, canteens etc., these are to prevent risk to security and / or health & safety of staff.
- The use of CCTV by staff will reduce the risk to the security, health & safety of such staff, where such usage is advised to those interacting with such staff.
- The purpose of CCTV in the public areas of our buildings is to enhance security and health and safety for all users of the buildings.
- Within meeting rooms CCTV is used to ensure the security and health and safety of staff when meeting / interviewing visitors and customers.
- The use of CCTV on streets and public areas is to act as a deterrent against anti-social behaviour and crime in town areas and at specific locations.

## 8. Locations of Cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy will not take place. Cameras placed to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

## 9. CCTV Video Monitoring and Recording

CCTV video monitoring and recording may include the following:

- Protection of Council buildings and property: The building's perimeters, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services, customer service areas and meeting rooms
- Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas
- Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms
- Video Patrol of Public Areas: Parking areas, main entrance /exit gates, Traffic Control
- Criminal Investigations
- Investigations carried out by other agencies

## 10. Covert Surveillance

Fingal County Council will not normally engage in covert surveillance. However, such surveillance may on occasion be required and justified where overt surveillance would merely transfer any illegal activity to some other location where CCTV is not in place. For example, illegal dumping at specific locations could justify covert surveillance, subject to this policy.

Where An Garda Síochána requests to carry out covert surveillance in Council property, any request will be in writing.

## 11. Notification & Signage

The Council will place this policy on its Intranet for the information and adherence of staff and on its website for the information of the public.

Adequate CCTV signage will be placed at locations where CCTV camera(s) are sited, including at entrances to Council offices and property as well as advance notices

indicating the use of CCTV. Signage may include the name and contact details of the Council's Data Controller as well as the specific purpose(s) for which the CCTV camera is in place in each location and any other information as required. Appropriate locations for signage may include:

- entrances to premises, i.e. external doors and entrance gates
- reception areas
- at or close to each internal camera

As part of this policy the Council may regularly publicise the fact that staff may use video and audio recording devices during the course of their work. Such staff, when using such equipment, must advise persons approaching them that the interaction is being recorded by way of video and audio.

**12. Storage & Retention**

Article 5 Section 1 (e) of the EU GDPR 2016/679 states that data *" kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.* This policy provides for a maximum retention period of 28 days, except where a need is identified that requires that such images / recordings are retained in relation to incidents / events. This time frame also complies with the guidelines issued by the Office of the Data Protection Commissioner.

The recordings, tapes, DVDs, servers etc. will be stored in secure environments with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the relevant designated / authorised persons. The Data Protection Officer will oversee arrangements but may delegate the administration of the CCTV System to other staff members.

**13. Access**

Unauthorised access to recordings, monitors etc. will not be permitted at any time. Monitoring stations will be kept locked. A log of access to monitoring stations and tapes, servers, DVDs etc. will be maintained. In relevant circumstances, CCTV footage may be accessed:

- by An Garda Síochána on request in writing when a crime or suspected crime has taken place and / or when it is suspected that illegal / anti-social

behaviour is taking place on Council property or in a public place or
- to other statutory bodies as deemed appropriate or
- to assist the Data Protection Officer, or relevant designated / authorised persons in establishing facts in cases of unacceptable behaviour or
- to data subjects (or their legal representatives), pursuant to an access request under the Data Protection Acts, where the time, date and location of the recordings is furnished to the Council or
- to individuals (or their legal representatives) subject to a Court Order
- to the Council's insurers where it requires same in pursuit of a claim for damage done to the Council's insured property

**14. Access Requests**

Under the Data Protection Acts, on written request, any person whose image may have been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image / recording exists, i.e. has not been deleted and provided also that an exemption / prohibition does not apply to the release.

Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that other persons are not identified or identifiable.

To exercise a right of access, a data subject must make an application in writing to the Data Protection Officer. Access requests can be made subject to the following:

- A person should provide all the necessary information to assist the Council in locating the CCTV recorded data, such as the date, time and location of the recording.
- If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be released by the Council.
- In seeking such an image, it will be necessary for the requester to submit their own photograph in order to ensure that it matches with that on the CCTV.
- In giving a person a copy of their data, the Council may provide a still / series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

**15. Audio Recordings**

The Council may provide audio recording systems in meeting rooms, phones systems or on staff directly, in conjunction with CCTV to enhance staff security in carrying out their statutory duties. Signage will be provided in such rooms and staff will advise customers and others that meetings are being audio / video recorded.

Audio recording will be deleted within 28 days, like that of video recordings in compliance with Section 12 above.

**16. Responsibilities**

The Data Protection Officer will:

- Ensure that the use of CCTV is implemented in accordance with the policy set down by Fingal County Council
- Oversee and co-ordinate the use of CCTV for safety and security purposes within Fingal County Council
- Ensure that all existing CCTV are evaluated for compliance with this policy
- Ensure that any new CCTV Systems installed are compliant with this policy and that Privacy Impact Assessments are undertaken where necessary
- Ensure that systems for access control, monitoring, recording and storage of cctv by the Council is consistent with the highest standards and protections
- Ensure that systems for the release of any information or recorded CCTV material stored comply with this policy
- Advise Departments on aspects of the deployment and location CCTV systems whether fixed or temporary
- Consider feedback / complaints regarding possible invasion of privacy or confidentiality due to the location of a CCTV camera or associated equipment

The relevant Designated / Authorised Person will:

- Ensure that the use of CCTV systems is implemented in accordance with this policy
- Co-ordinate the use of CCTV monitoring
- Ensure that the CCTV monitoring is conducted in line with this policy
- Ensure that any new CCTV Systems installed are compliant with this policy and undertake Privacy Impact Assessments where necessary
- 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 or any material recorded or stored in the system
- Ensure that monitoring recorded tapes are not duplicated for release

- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Provide a list of the CCTV cameras and the associated monitoring equipment and the capabilities of such equipment to the Data Protection Officer
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. NOTE: [Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by An Garda Síochána].
- Report on feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment to the Data Protection Officer
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the council and be mindful that no such infringement is likely to take place
- Co-operate with the Data Protection Officer and Health & Safety Officer of Fingal County Council in reporting on the CCTV system in operation
- Ensure that external 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 monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Director of Services
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas

**17. Security Companies**

The Councils CCTV, if controlled by a security company contracted by the Council, will comply with this policy and the following:

- The Council will ensure that it only contracts security firms which are

registered as either installers or monitors of CCTV under the Private Security Authority Act, 2004 as amended.

- The Council will have a written contract with the security company in place which details the areas to be monitored, how long data is to be stored, what the security company may do with the data, what security standards should be in place and what verification procedures apply.
- The written contract will also state that the security company will give the Council all reasonable assistance to deal with any subject access request made under Article 15 of the EU GDPR 2016/679 which may be received by the Council to ensure the release, by the Council, of the data within the statutory time-frame set out in Artcile 12 Section 3 of the EU GDPR 2106/679 *" without undue delay and in any event within one month of receipt of the request".*

Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors." As data processors, they operate under the instruction of data controllers (their clients). Section 28 of the EU GDPR 2016/679 places a number of obligations on data processors. These include:

- Having *appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*
  *And*

  (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
  (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
  (c) takes all measures required pursuant to Article 32;
  (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
  (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
  (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
  (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
  (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

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. Staff of the security company must be made aware of their obligations relating to

the security of data.

## 18. Implementation & Review

This 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), legislation and feedback from staff and others.

Implementation of and adherence to the policy to be monitored by the Data Protection Officer and reported to the Council's Executive Management Team.

Document Control

| | | | |
|---|---|---|---|
| **Document Ref:** | FCC/GDPR/POL/CCTV/002 | **Title:** | Fingal CCTV Policy |
| **Version& Date:** | 2 | **Author:** | Colm McQuinn, |

| | | | |
|---|---|---|---|
| | 20/08/2018 | | DPO |
| **Directorate:** | Corporate Affairs & Governance | **Department:** | Data Protection Office |
| **Changes reported to Management Team** | | **Date** | |
| **Reviewed:** | | **Change History** | |

**APPENDIX I – DEFINITIONS.**

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

**Access Request** – This is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and / or Section 4 of the Data Protection Acts.

**Audio recording** - The use of equipment for recording of voice and sound.

**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. It includes in this policy the recording of sound.

**Data** - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

**Data Controller** - a person who (either alone or with others) controls the contents and use of personal data.

**Data Processing** - performing any operation or set of operations on data, including:

Obtaining, recording or keeping the data - Collecting, organising, storing, altering or adapting the data - Retrieving, consulting or using the data - Disclosing the data by transmitting, disseminating or otherwise making it available - Aligning, combining, blocking, erasing or destroying the data

**Data Processor** - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work.

**Data Subject** – an individual who is the subject of personal data.

**Personal Data** – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.