2020

CCTV & Audio Recording Policy and Procedure

Document Version Number:	2.1
Issue Date:	Dec 2020

Comhairle Cathrach Chorcaí
Cork City Council

Table of Contents

Revision History

CURRENT DOCUMENT VERSION		
Version No:	**Date:**	**Reasons for Issue:**
2.1	**February 2021**	**Community CCTV addition**

REVISION APPROVAL			
Process Owner	**Signature:**	**Print Name:**	**Date:**
	Data Protection Officer		Dec 2020
GDPR Group	**Signature:**	**Print Name:**	**Date:**
SMT Approval	**Signature:**	**Print Name:**	**Date:**
		Paul Moynihan	23rd February 2021

PREVIOUS VERSIONS		
Version No.	**Date**	**Reason for Issue**
1.0	**May 2018**	**GDPR Guidelines**
2.0	**June 2019**	Updated
2.1	**Nov 2020**	Community CCTV

1. Introduction/Background

CCTV captures personal data of individuals i.e images of persons and other personal data.
CCTV in a public place is considered to represent a high risk to the rights and freedoms of individuals under data protection legislation.
City Council is obliged to protect such data in accordance with provisions contained in the General Data Protection Regulation (GDPR) which came into effect on 25th May 2018 and the Data Protection Acts 1988- 2018.

Cork City Council currently operates two types of CCTV systems : Private and Public.

Private CCTV Systems operate at premises such as Council buildings, fire stations, libraries, operational depots and other locations where the public do not have a right of access, either implied or express. While there may be some capture of persons passing by these buildings they are considered to be private and do not require the consent of the Garda Commissioner.

Public CCTV Systems operate in public places such as parks, walkways, cemeteries, on streets, on roadways, bridges, at bring centres and other public places where the public has either an implied or express, right of access .Locations within Council premises such as reception areas and corridors to which the public has access as well as buildings open to the public are considered public places.

This document sets out Cork City Council's Policy in relation to the use of Closed Circuit Television Systems (CCTV) and should be read in conjunction with the guidance provided by Data Protection Commissioner.

DPC Guidance on CCTV

2. Purpose of Policy & Procedure

The purpose of this policy is to outline specific provisions to assist Cork City Council to fulfil its data protection obligations regarding the operation of CCTV systems including, but not limited to, the application process and approval, arrangements relating to the location, monitoring, control and security of CCTV systems, recording by CCTV systems and access to recordings.

3. Reasons for CCTV Video Monitoring and Recording

CCTV in this policy refers to video recording and audio recording systems and may be used for the following purposes:

- To protect and safeguard the health and safety of Cork City Council staff, Elected Members, customers, visitors and contractors;
- To safeguard and protect the security of premises both internally and externally and the plant, equipment and property, parks and cemeteries and all other assets under the ownership and remit of Cork City Council;
- To secure public order and safety in public places;
- To help create a cleaner environment and public spaces by identifying and combating illegal dumping;
- To help with better traffic management and control, traffic counting and categorisation, traffic flow;
- To improve public and community safety and perception of safety by the local communities by facilitating the deterrence, prevention, detection and prosecution of offences, assisting in identifying, apprehending and prosecuting offenders;
- To prevent, detect and investigate crime and illegal activities, i.e. littering and the prosecution of offences arising from same;
- Criminal Investigations by An Garda Síochána,
- Investigation by Cork City Council management of reported incidents/accidents and of suspected, or allegations of fraudulent behaviour or other activities consistent with this policy.
- Investigations carried out by other agencies in relation to incidents in the above locations, i.e. Health and Safety Authority, Cork City Council's Insurers and or legal advisors.
- Raising awareness for members of the public interacting with staff that their actions are being recorded in order to deter offences.

Cork City Council considers that the use of CCTV in the above circumstances to be appropriate.

CCTV will not be used by Cork City Council to monitor employee performance and any information obtained in violation of this policy in relation to employee performance cannot be used in any disciplinary proceedings against any employee of the Council.
It may however, on specific occasions, be used in the investigation of complaints.

4. Scope

The scope of this policy document applies to all:

- Cork City Council employees but especially data users
- Cork City Council uses of CCTV that involve the recording of personal data.
- CCTV service providers (data processors) contracted by Cork City Council.

5. Definitions

For the purposes of this policy, the following terms have the following meanings:

"**CCTV":** means Closed Circuit Television Systems which are fixed and domed cameras designed to capture and record images of individuals and property.
"**Data**": is information which is stored electronically, or in certain paper-based filing systems.In respect of CCTV, this generally means video images.
"**Data controllers**": are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law.
"**Data processors**": means any person or organisation that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).
Data subjects": means all living individuals about whom we hold personal information as a result of the operation of our CCTV (or other surveillance systems).
"**Data users**": are those employees whose work involves processing personal data.
This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy.
"**Personal data**": means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.
"**Processing**": is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

6. Roles & Responsibilities

All staff involved in the proposed installation or already installed CCTV systems are responsible to ensure use of CCTV is in accordance with this policy and guidance from the Data Protection Commissioner.

The relevant Director of Services or their designated staff members have responsibility for:

- Ensuring the operation of existing CCTV systems within their areas of responsibility is consistent with the highest standards and protections and that they are operated in

accordance with this policy and relevant legislation.

- Ensuring that any proposals in relation to the provision of new CCTV schemes are processed In accordance with the checklist at Appendix II

- Assigning responsibility for specific CCTV and the day to day operation and maintenance of systems to suitable members of staff .

- Ensuring that images recorded on tapes/DVDs/digital recordings are stored for periods of no 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.
- Ensuring that arrangements are in place with contractors/third parties in accordance with Section 19 of this policy.
- Ensuring that DVRs, servers, tapes, DVDs' etc., are stored in a secure place with access restricted to authorised personnel only.
- Ensuring that all requests received for access to data are directed in the first instance to the Data Protection Officer.

- Ensuring that a record of access to (i.e. an access log), and/or a record of the release of any material is maintained.

- Arranging for an evaluation of existing CCTV systems to be carried out on an annual basis.

- Carrying out a Data Privacy Impact Assessment (DPIA) in advance of any new CCTV scheme or replacement cameras .

7. DPIA

In line with of Article 35 of the GDPR and DPC guidance relating to the use of CCTV a Data Protection Impact Assessment (DPIA) must be carried out before any installation of a new CCTV system. A DPIA may also be required for upgrade to an existing CCTV system if in the opinion of Cork City Council, the installation or upgrade is likely to result in a high risk to the rights and freedoms of individuals. The purpose of a DPIA will be to facilitate the identification and implementation of appropriate measures to eliminate or minimise any risks arising out of the processing of personal data by a CCTV system

A draft DPIA must be submitted to the Data Protection Officer for review and final DPIA signed off by the relevant Director of Services.

DPIA's should be reviewed every 3 years (as per DPC Guidance)

8. Community Based CCTV

Section 38 of the Garda Síochána Act 2005 provides that the Garda Commissioner may authorise the installation and operation of CCTV for the sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences (commonly referred to as Community Based CCTV Schemes). The criteria to be met for Community Based CCTV Schemes are set down in statutory instrument S.I. 289 of 2006. In addition, a 'Code of Practice for Community Based CCTV Systems' has been developed and published jointly by the Department of Justice and Equality and An Garda Síochána. The following conditions are required to be met in order to obtain authorisation from the Garda Commissioner:

- The CCTV scheme must be approved by the local authority after consultation with the joint policing committee for its administrative area;
- The CCTV scheme must comply with technical specifications issued by the Garda Commissioner and be operated in accordance with the Code of Practice;
- Members of An Garda Síochána will be given access at all times to the CCTV system upon request;
- The local authority gives an undertaking that it will act as a Data Controller in respect of the CCTV system.

Cork City Council currently has 1 Community CCTV Scheme in operation in Blackpool.

Code of Practice 2019

Community CCTV Application Form

9. CCTV Locations

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals have a reasonable expectation of privacy is prohibited. Cameras placed so as to record external/internal areas must be positioned in such a way as to prevent or minimise the recording of passers-by or of another person's private property.

Video monitoring of public areas and within Cork City Council's public offices & premises for security and health and safety purposes, is restricted 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 privacy such as break rooms, changing rooms, showers and toilets.

10. CCTV Signage

Cork City Council will ensure that adequate CCTV signage is 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 includes the name and contact details of the Data Controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

Corporate signage is available from the DPO.

11. Covert CCTV Surveillance

The use of CCTV to obtain data without an individual's knowledge is generally unlawful. However Cork City Council may, on occasion, engage in covert surveillance.

Such surveillance will only be used on an exceptional case by case basis where the data is collected and retained for the purposes of preventing, detecting or investigating offences or apprehending or prosecuting offenders. Examples of such circumstances may include litter, graffiti and waste enforcement among others.

The decision to utilise covert surveillance must be carried out in accordance with this policy and approved in advance by the relevant Director of Service. The use of covert CCTV may result in the initiation of legal proceedings. The recommendation to proceed with covert CCTV for this purpose must be supported by documentary evidence of the incidents which has led to the decision to proceed with same. This should be contained in the Data Privacy Impact Assessment (DPIA.)

Covert surveillance is to be focussed and of a short duration, not exceeding 4 weeks. Only specific and relevant locations/individuals will be recorded. If no evidence is obtained, surveillance should cease.

The Data Protection Officer must be notified in advance of any planned covert surveillance.

12. Retention of CCTV recordings

Data recorded on CCTV systems shall be kept for no longer than is considered necessary.. The Data Protection Acts 1988 to 2018 states that ***"the data shall be kept in a form .....for no longer than is necessary for the purposes for which the data are processed".***

This policy provides for a maximum retention period of no longer than 28 days, except where the images identify a specific issue – such as a break-in or theft or required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use. In those instances, these images / recordings may be retained beyond the 28 days. This time frame of 28 days complies with the guidelines issued by the Office of the Data Protection Commissioner.

13. CCTV Security Arrangements

The recordings, tapes, DVRs , DVDs', servers etc. must be stored in secure environments and restricted to authorised personnel only.

A log of access to monitoring stations , servers, dvds must be maintained

14. Access to CCTV Recordings

All requests for access to CCTV data must be channelled through the Data Protection Officer in the first instance .

Access may only be provided to the following:

1. A Data Subject
2. An Garda Síochána
3. Other third parties ie Cork City Council's insurers

1. Access by Data Subjects

Data protection legislation provides data subjects with a right to access their personal data. This includes their recognisable images and other personal data captured by CCTV recordings. Access requests are encouraged to be made with the Data Subject Access Request Form ,however requests made in writing/by email will also be accepted provided all necessary information is supplied .
In seeking 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, Cork City Council may provide a copy of the footage in video format or where it is not technically possible to do so, provide a still or series of still pictures, a tape or a disk with relevant images.

If the image is of such poor quality so as not to clearly identify an individual, that image may not be considered to be personal data and may not be released by Cork City Council.

If there are images and/or other personal data of other individuals(not the data subject) on the recording these must be obscured/pixellated before the data is released unless consent has been obtained from those other parties to their release.

If the CCTV recording no longer exists on the date that Cork City Council receives an access request it will not be possible to provide access to a data subject.

2. **Access by An Garda Síochána –**

There is a distinction between a request by An Garda Síochána to view CCTV recordings and a request to download/obtain copies of such recordings

Request to view - In general, a request made by An Garda Síochána to simply view CCTV recordings should be accommodated as it does not raise any concerns from a data protection perspective. All such requests must be entered in the access log.

Request for copy of recording/download - The handing over /downloading of CCTV footage to An Garda Síochána requires a formal written communication confirming that the material is sought for the prevention, investigation or detection of a crime.

AGS Request to download CCTV form.

Emergency requests – In order to expedite a request in urgent situations, a verbal request from An Garda Síochána for copies of CCTV recordings will suffice. This should only happen in exceptional circumstances. However, such a verbal request must be followed up with a formal written request from An Garda Síochána.

3. **Access by other 3rd Parties**

Access by third parties such as public bodies, private organisations and individuals other than the data subject to CCTV recordings will only be provided in circumstances that are permitted by data protection legislation.

15. Complaints To Data Protection Commissioner

Data subjects may make a complaint to the Data Protection Commissioner in the following circumstances:

- If they experience a delay outside of the prescribed timeframe for making a decision on an access request or if they are dissatisfied with a decision by Cork City Council on their access request;
- If they consider that Cork City Council's processing of their personal data is contrary to their data protection rights.

Contact details for the Data Protection Commission are as follows:

16. CCTV Register

A CCTV Register shall be maintained by Cork City Council's Data Protection Officer. This register shall contain the following information:

- Location of each CCTV system.
- Purpose of each CCTV system.
- CCTV service provider details.
- Signage.
- Details of Designated Employee having responsibility for each CCTV system.
- Details of personnel having authorised access to each CCTV system.
- Retention period for CCTV recordings.

17. Access Log

The Director of Service/Designated Staff Members must ensure that the authorised removal and/or viewing of data is documented by the recording of the following in an access log:

- Date and time when the images were removed from the system or viewed;
- The reason why the images were removed from the system or viewed;
- Any crime incident number to which the images may be relevant;
- The location of the data images;
- The name(s) of the person(s) viewing the images. (If this should include third parties, the name of the organisation to which the third party belongs);
- The signature of the collecting official, where appropriate, and the signature of the official signing out the data;
- The extent of the information to which access was allowed or which was disclosed;
- The outcome, if any, of the viewing;
- The date and time the images were returned to the system or secure place, if they have been retained for evidential purposes.

CCTV ACCESS REQUEST LOG

18. Data Processors- Security Companies

Article 28 of the GDPR places a number of obligations on Data Processors.
Security companies that place, operate and or monitor CCTV cameras on our behalf are considered to be "Data Processors." As Data Processors, they operate under our instructions as the data controller.

Cork City Councils' CCTV, if controlled by a security company contracted by the Council will comply with this policy.

Directors of Services/ Designated Staff Members must ensure that only security firms which are registered as either installers or monitors of CCTV under the Private Security Authority Act 2004 as amended are contracted.

Directors of Services/ Designated Staff Members must ensure that all security companies who process data on behalf of Cork City Council will be required to sign a Data Processing Agreement(DPA). CCC Data Processing Agreement

19. Roles and Responsibility

The relevant Director of Services or their designated staff members have responsibility for:

- Ensuring the operation of existing CCTV systems within their areas of responsibility is consistent with the highest standards and protections and that they are operated in accordance with this policy and relevant legislation.
- Ensuring that any proposals in relation to the provision of new CCTV schemes are processed in accordance with the checklist in Appendix 11.
- Assigning responsibility for specific CCTV and the day to day operation and maintenance of systems to suitable members of staff .
- Ensuring that images recorded on tapes/DVDs/digital recordings are stored for periods of no 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.
- Ensuring that arrangements are in place with contractors/third parties in accordance with this policy.
- Ensuring that DVRs, servers, tapes, DVDs' etc., are stored in a secure place with access restricted to authorised personnel only.
- Ensuring that all requests received for access to data are directed in the first instance to the Data Protection Officer .
- Ensuring that a record of access to (i.e. an access log), and/or a record of the release of any material is maintained.
- Arranging for an evaluation of existing CCTV systems to be carried out on an annual basis.
- Carrying out a Data Privacy Impact Assessment (DPIA) in advance of any new CCTV scheme or replacement cameras .

20. Review

This policy will be reviewed annually by the DPO and GDPR Implementation Team taking cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, An Garda Síochána, etc).

21. Communications Plan

Cork City Council will circulate this policy to all staff and place it on the Intranet.
It will also be published on Cork City Council's website at www.corkcity.ie for the information of the public.

22. Appendix I – Change Log

23. Appendix II – DPC CCTV Checklist

New CCTV systems or replacement /upgraded cameras

Directors of Service and Heads of Function are responsible for ensuring that any proposals in relation to the provision of new CCTV schemes are processed in accordance with the terms of this policy and taking account of the checklist issued in May 2019 by the Data Protection Commissioner.

CCTV Checklist

Purpose: Do you have a clearly defined purpose for installing CCTV? What are you trying to observe taking place? Is the CCTV system to be used for security purposes only? If not, can you justify the other purposes? Will the use of the personal data collected by the CCTV be limited to that original purpose?

Lawfulness: What is the legal basis for your use of CCTV? Is the legal basis you are relying on the most appropriate one?

Necessity: Can you demonstrate that CCTV is necessary to achieve your goal? Have you considered other solutions that do not collect individuals' personal data by recording individuals' movements and actions on a continuous basis?

Proportionality: If your CCTV system is to be used for purposes other than security, are you able to demonstrate that those other uses are proportionate? For example, staff monitoring in the workplace is highly intrusive and would need to be justified by reference to special circumstances. Monitoring for health and safety reasons would require evidence that the installation of a CCTV system was proportionate in light of health and safety issues that had arisen prior to the installation of the CCTV system. Will your CCTV recording be measured and reasonable in its impact on the people you record? Will you be recording customers, staff members, the public? Can you justify your use of CCTV in comparison to the effect it will have on other people? Are you able to demonstrate that the serious step involved in installing a CCTV system that collects personal data on a continuous basis is justified? You may need to carry out a Data Protection Impact Assessment to adequately make these assessments.

Security: What measures will you put in place to ensure that CCTV recordings are safe and secure, both technically and organisationally? Who will have access to CCTV recordings in your organisation and how will this be managed and recorded?

Retention: How long will you retain recordings for, taking into account that they should be kept for no longer than is necessary for your original purpose?

Transparency: How will you inform people that you are recording their images and provide them with other information required under transparency obligations? Have you considered how they can contact you for more information, or to request a copy of a recording?

If, having examined all other alternatives, it is considered that additional CCTV systems are the only suitable solution available; then an assessment of the impact of the proposed system on the privacy of individuals (Data Privacy Impact Assessment) must be carried out

by the relevant section and the principle of “Privacy by Design” incorporated into the development of same.
Supporting documentation on a decision to proceed with a new CCTV system must be retained for review and inspection as appropriate.

If the DPIA indicates that the data processing risk is a high risk which cannot be sufficiently addressed, the Office of the Data Protection Commissioner must be consulted to seek its opinion as to whether or not the processing operation complies with legislation.

In the event that no risk is identified or the risk is considered to be a low risk, then the decision to proceed with any new CCTV schemes will require the approval of the relevant Director of Services.