Comhairle Cathrach
& Contae **Luimnigh**

Limerick City
& County Council

CCTV Policy

Contents

Document Control

Document Location

Limerick City and County Council Website and Staff Portal

Revision History

Date of this revision: May 2022	**Date of next review: May 2023**

Version Number/Revision Number	**Revision Date**	**Summary of Changes**
2.0	May 2022	Complete revision of CCTV policy to include the following: Document Structure, condensed version of existing policy with some sections removed as they were not relevant. Established the role of CCTV Oversight Board and updated other roles within the policy.

Consultation History

Revision Number	**Consultation Date**	**Names of Parties in Consultation**	**Summary of Changes**
2.0	July 2022	Senior Forum and Mgt Team	Complete revision of existing policy
1.0	Dec. 2019	Limerick Joint Policing Committee	Initial CCTV Policy approved

Approval

This document requires the following approvals:

Name	**Title**	**Date**
	Management Team	10/06/2022
	Senior Forum	07/06/2022
	Limerick Joint Policing Committee	12/12/2019

This policy shall be reviewed on an annual basis by the Head of Digital Strategy in consultation with the DPO.

1. Introduction/Background

This document sets out Limerick City and County 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. Click Here to Access DPC Guidance on CCTV

Limerick City and County Council (the "**Council**") is the authority responsible for local government in the City and County Limerick in Ireland. It came into operation on 1st June 2014. It was formed as the result of a merger of Limerick City Council and Limerick County Council under the provisions of the Local Government Reform Act 2014. The corporate headquarters are based at Merchants Quay, Limerick, V94 EH90.

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.

The Council, as Data Controller, 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 2018.

The Council currently operate CCTV systems for two distinct purposes: Community CCTV Schemes and Property security.

Community CCTV Systems operate in public places such as walkways, on streets, on roadways, bridges, at city centres and other public places where the public has either an implied or express, right of access. A proportion of our Community CCTV Systems are real-time monitored by a third-party services provider at a dedicated monitoring centre. https://www.limerick.ie/council/services/your-council/digital-services/limerick-city-and-county-council-cctv-policy-cctv
Retrospective monitoring is carried out upon request from An Garda Síochána or in receipt of a valid data access request.

Property CCTV Systems operate at or in premises such as Council buildings, fire stations, libraries, operational depots and other Council owned locations. Property CCTV Systems are also operated at locations within Council premises such as reception areas and corridors to which the public has access, as well as in buildings open to the public.

2. Purpose of Policy

The purpose of this policy is to

- outline why and how the Council uses CCTV, and how the Council will process data recorded by CCTV cameras;
- ensure that the legal rights of individuals whose images are recorded by the Council's CCTV systems, relating to their personal data, are recognised and respected;
- assist staff in complying with their own legal obligations when working with personal data;
- explain how individuals can exercise their rights in respect of personal data created by the Council's CCTV Systems.

3. Reasons for CCTV Video Monitoring and Recording

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

- To protect and safeguard the health and safety of 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 the Council
- To assist in the maintenance of public order and safety in public places
- To improve public and community safety and perception of safety by the local communities by assisting in the prevention, detection and investigation of offences, in turn assisting in the prosecution of offenders
- To prevent, detect and investigate crime and illegal activities and in order to assist in the prosecution of offences
- Criminal Investigations by An Garda Síochána (AGS)
- Investigation by 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, i.e. Health and Safety Authority, the 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, e.g. assault and bodily harm

The Council considers that the use of CCTV in the above circumstances to be both necessary and proportionate for the achievement of those purposes.

CCTV will not be used by the Council to monitor employee performance. It may however, on specific occasions, be used in the investigation of complaints and for disciplinary matters.

For the avoidance of doubt, CCTV monitoring/profiling of an individual based on any of the following characteristics is prohibited by this policy;

- Age
- Civil status
- Disability
- Family status
- Gender
- Race
- Religion
- Sexual orientation
- Membership of the Travelling Community

4. Scope

This policy document applies to all:

- Council employees but especially Data Users (as defined below);
- CCTV service providers (data processors) contracted by the 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 Pan-Tilt-Zoom (PTZ) cameras designed to capture and record images of individuals and property.

"CCTV Officer": employee of the Council who is authorised to access CCTV footage for specific purposes.

"Council": means Limerick City and County Council.

"**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.

"**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

The responsibility for CCTV is delegated to:

- *The CCTV Oversight Board* - a cross-departmental working group established by the Council's Management Team to support the implementation of the CCTV Strategy. The CCTV Oversight board is a sub group of the Data Protection Monitoring Committee. The Chair of the CCTV Oversight Board reports to the Data Protection Monitoring Committee and Senior Management team.

- *The CCTV Co-ordinator* - reporting to the CCTV Oversight Board, responsible for the daily operations of the CCTV systems in line with this policy.

- *Data Protection Officer* - appointed by the Council, who will monitor compliance with the Council's data protection obligations concerning the operation of its CCTV Systems.

- *Head of Digital Strategy* - is the owner of this document and is responsible for ensuring that this policy is reviewed in line with the requirements stated within this document.

CCTV Oversight Board

The CCTV Oversight Board is a cross-departmental working group responsible for co-ordinating the use of CCTV in the Council. The broad remit of the CCTV Oversight Board is to support the Chair of the Oversight Board in providing overall direction and management for CCTV projects according to the overall CCTV Strategy and to make key decisions including commitment of resources. Any future proposed changes as deemed necessary by AGS or the Council in relation to cameras must be considered by the CCTV Oversight Board. The DPO is consulted as a member of the Oversight Board. The CCTV Oversight Board will meet bi-annually to review the live monitoring status of cameras. The Board have committed to review all cameras and their functionality on an annual basis. The CCTV Oversight Board structure consists of:

CCTV Oversight Board Sponsors:

- Director of Services, Regeneration
- Director of Services, Housing
- Director of Services, Economic Development & Enterprise
- Director of Services, Support Services

CCTV Oversight Board Members:

- Head of Digital Strategy
- Data Protection Officer
- Senior Executive Engineer, Regeneration
- Senior Engineer, Housing
- Independent individual

The members of the CCTV Oversight Board are obliged to:

- Review CCTV related policies and standards
- Agree cross-departmental funding of CCTV function
- Authorise and prioritise CCTV projects
- Conduct an annual audit of all CCTV locations, processes and procedures
- Meet bi-annually to review the live monitoring status of cameras

Live Monitoring Asset Review

Bi-annually, the CCTV Oversight Board will review the live monitoring status of cameras. A determination will be made as to which cameras should continue to be live monitored and which cameras should no longer be monitored.

On occasions when not being actively monitored by an operator, all operating cameras should be placed in the most advantageous position to record any incidents occurring in a public area within its field of vision.

CCTV Co-ordinator

The CCTV Co-ordinator reports to the CCTV Oversight Board and is responsible for the daily operations of the CCTV systems in line with this policy. The CCTV Coordinator monitors the operation of the CCTV system and cameras on an ongoing basis and calls upon the contractor as required.

The main duties and responsibilities are to:

- Ensure that the use of CCTV is implemented in accordance with this policy
- Oversee and co-ordinate the use of CCTV for safety and security purposes within the Council
- Maintain the list of CCTV installation requests, internal and external, and make recommendations for new camera installations in line with the CCTV strategy and CCTV policy
- Liaise with the DPO regarding the CCTV Officers List
- Maintain the CCTV Access Procedure
- Ensure that the CCTV installations are compliant with this CCTV policy
- Ensure that all existing CCTV are evaluated for compliance with this policy
- Maintain the CCTV asset register
- Ensure that the CCTV monitoring by the Council is consistent with the highest

standards and protections

- Co-ordinate and support the release of recorded CCTV data in compliance with this policy and data protection legislation
- Maintain a record of access (i.e., an access log) to, or the release of footage or any material recorded or stored in the system
- Ensure that no copies of recordings are made without authorisation
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Ensure that all areas being monitored are not in breach of an expectation of the privacy of individuals and be mindful that no such infringement is likely to take place
- Advise, in conjunction with the DPO, on the Council's cameras (excluding Community CCTV Scheme cameras) to ensure they 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 CCTV footage is stored in a secure place with access by authorised personnel only
- Ensure that images recorded are stored for a period 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 as approved by the CCTV Oversight Board
- Ensure that all financial obligations for operations and maintenance are traceable and auditable
- Consult with the DPO when appropriate

7. DPIA

A Data Protection Impact Assessment (**DPIA**) is undertaken in advance of installing or making adaptations to CCTV systems. 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 the final DPIA signed off by the relevant Director of Services/Head of Section.

DPIA's should be reviewed at least every 3 years or more often, as appropriate (as per DPC Guidance).

8. Business case Rationale

For all new CCTV Installations, requests submitted to the CCTV Oversight Board must include a business case approved by the Director of Service requesting the installation as project sponsor and allocation of capital funding for installation and annual funding for maintenance, communications and monitoring costs for at least 5 years. The business case must also be approved by the Head of Finance or a nominated officer.

9. 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). An Garda Síochána are joint controllers of all cameras authorised under Section 38 of the Garda Síochána Act 2005. 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
- A submission and presentation must be made to AGS CCTV Advisory Committee that consists of three Chief Superintendents working in specialised areas and the DPO of AGS. At this meeting, AGS will either approve or decline the application, or make a request for updates or additional information, pending approval
- Members of An Garda Síochána will be given access at all times to the CCTV system upon written request in accordance with the agreed procedures
- The local authority gives an undertaking that it will act as a joint controller in respect of the Garda authorised and approved Community Based CCTV Schemes

10. CCTV Complaints

Complaints with regard to all Council CCTV systems should be directed to the Data Protection Officer in the first instance.

11. 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. CCTV will be utilised in a fair and ethical manner. The Council has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras are positioned in such a way as to prevent or minimise the recording of such places to the greatest extent possible. Privacy masking is applied on CCTV cameras, where necessary, in order to block-out areas where individuals have a reasonable expectation of privacy. In any area where CCTV is in operation, there will be a prominent sign displayed notifying people of same.

Community CCTV Scheme Locations

Section 38 of the Garda Síochána Act, 2005 lays down the conditions governing the operation of CCTV schemes in a public place. This includes the need for all CCTV schemes operating in public areas to have written authorisation of the Garda Commissioner. Section 38(1) provides as follows: "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."

Where a need is identified, the camera may only be deployed if it is assessed as being justified, necessary and proportionate in balancing the protection of the public with the rights of individuals and individual expectations of privacy, as part of a Data Protection Impact Assessment and taking into account the principle of data minimisation.

12. CCTV Signage

The Council will ensure that adequate CCTV signage is placed at locations where CCTV camera(s) are sited. Signage is clearly visible and legible to members of the public and includes the name and contact details of the Data Controllers as well as the specific purpose(s) for which the CCTV camera is in place in each location. Corporate signage is available from the Data Protection Officer. Appropriate locations for signage include:

- At or close to each camera
- Entrances to premises, i.e., external doors and entrance gates
- Reception areas
- Main entrances into cities and towns or villages
- Any other areas covered by CCTV

The Council will publish this policy on its Intranet for the information and adherence of staff and on its website https://www.limerick.ie/cctv-policy for public awareness and information.

13. Covert CCTV Surveillance

The use of CCTV to obtain data without an individual's knowledge is generally unlawful. However, the Council may, in exceptional circumstances, engage in covert surveillance. Such surveillance will only be used on an exceptional case by case basis where the Council has identified a legal basis to do so and where the Council considers that less intrusive means would not be sufficient for its purposes.

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 have led to the decision to proceed with same.

Covert surveillance is to be focussed, and of a short duration. Only specific and relevant locations/individuals will be recorded. Limited numbers of people will be involved in any covert surveillance.

The Data Protection Officer must be consulted in advance of any planned covert surveillance and the operation of any such covert surveillance will be subject to a Data Protection Impact Assessment prior to commencement of processing.

14. CCTV Retention

Article 5(1)(e) of the General Data Protection Regulation states that data shall be kept "for no longer than is necessary for the purposes for which the personal data are processed".

For both Community CCTV Systems and Property CCTV Systems in the Council - a retention period of 28 days applies, unless there are specific, legitimate and reasonable grounds for the retention of images beyond that period. At the end of their retention period, recordings and images will be erased permanently and securely. Any physical matter will be disposed of as confidential waste.

15. CCTV Security Arrangements

CCTV footage must be stored in secure environments and access will be restricted to authorised personnel only.

An access log must be maintained and made available for inspection on request from the Data Protection Officer.

Supervising the access and maintenance of the CCTV System is the responsibility of the CCTV Co-ordinator and CCTV Officers.

In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data where it is possible to do so.

The Council shall ensure that appropriate access controls are put in place in respect of image storage including robust encryption where remote access to live recording is permitted.

The Council will ensure staff are given appropriate training to ensure they understand and observe the legal requirements relating to the processing of data by the Council's CCTV Systems.

16. Accessing and Downloading CCTV Footage

Data will only be shared with third parties where the Council has a lawful basis to do so and only in accordance with this policy. We will maintain a record of all disclosures of CCTV footage. No images from CCTV will ever be posted online or disclosed to the media. Access may be provided to the following:

1. A Data Subject
2. An Garda Síochána
3. CCTV Officers of the Council
4. Other third parties where appropriate i.e., for example, the Council's insurers and/or legal advisors
5. Monitoring Service Provider and IT Support/Maintenance Providers
6. Other parties where the data subject gives his/her consent or instructs us to do so or where we are otherwise legally required to do so (e.g. on foot of a Court Order)

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 (See Appendix II), however requests made in writing/by email/verbally will also be accepted provided all necessary information is supplied. However, where an access request is made verbally, the Council's Data Protection Officer would encourage individuals to submit email/ written access requests where practical, to avoid disputes over the details, extent, or timing of an access request. In seeking an image, it will be necessary for the requester to submit their own photographic ID in order to ensure that it matches with that on the CCTV recordings.

In giving a person a copy of their data, the 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 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 the 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 the Council receives an access request it will not be possible to provide access to a data subject.

Access by An Garda Síochána to Community CCTV Schemes and Property Security CCTV

Request for copy of recording/download or viewing -

The viewing/handing over/downloading of CCTV footage to An Garda Síochána requires a formal written communication (CCTV Access Request protocol form) confirming that the material is sought for the prevention, investigation or detection of a crime. A log of all An Garda Síochána requests must be maintained. Any such requests should be on An Garda Síochána headed paper, quote the PULSE unique number, the details of the CCTV footage required and should also cite the legal basis for the request. The request form must be signed by a member of Superintendent or Inspector rank to authorise

the request. Where any such requests are made directly to the data processor instead of the Council, the processor maintains a log and upon request provides a copy to the Council. This log is available for inspection at all times.

Emergency requests – In order to expedite a request in urgent situations, a verbal request from An Garda Síochána to access 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. The request form must be signed by a member of Superintendent or Inspector rank.

Access by CCTV Officers

CCTV footage can only be accessed by designated Council staff members who are known as 'CCTV Officers'. To become a CCTV Officer, the following steps must be taken:

- Seek approval from a Director of Service
- Approval to be forwarded to the Data Protection Officer
- The CCTV Oversight Board will review the CCTV Officers designation annually and will re-certify the members as appropriate
- In order to access Community CCTV Schemes, designated staff members must be non-Act Garda vetted. Please contact the Data Protection Officer to commence this process

CCTV Officers are authorised to view CCTV footage. Downloading of footage requires an access form to be completed and the access must be approved and logged with the Data Protection Officer. Any such requests should be on Council headed paper, details of the CCTV footage required and should also cite the legal basis for the request, i.e. the Act, Section, etc. under which the request is made. The requester must ensure that the request complies with: Data Protection Legislation, the underlying legislation under which the request is made and this CCTV policy.

The DPO will approve the CCTV Download Request (See Appendix III) and return the signed CCTV Download Request to the CCTV Officer only when satisfied that all the conditions have been met. The CCTV Officer must keep a copy of the approved CCTV download request in the inspection record and present the original approved CCTV request to the monitoring Centre in order to obtain the footage.

The monitoring centre must retain the original signed CCTV download request for a period of no less than 5 years.

For audit and verification purposes a record must be maintained by the Council on all CCTV download requests regardless of whether they are approved or not.
The DPO will report to the CCTV Oversight Board on an annual basis:

- Total Number of CCTV download requests
- Number of CCTV download requests approved
- Number of CCTV download requests rejected

Third Parties

From time to time the Council shares CCTV recordings with its advisors, for example, its insurers and its legal advisors for the purposes of obtaining legal advices, resolving disputes and defending, compromising or otherwise settling litigation.

Monitoring Services and IT Support/Maintenance Providers

The Council shares CCTV footage with third party services providers, as data processors, to assist the Council with the administration and maintenance of the CCTV system and associated hardware and software.

Other Parties

Where a data subject gives consent or instructs the Council to do so (e.g. to your solicitor, to your union representative etc.), or where we are otherwise legally required to do so (e.g. on foot of a Court Order).

Visitors to the CCTV Monitoring Centre are permitted only with the prior written approval, and in the presence of the CCTV Projects Co-ordinator or a staff member as nominated by the CCTV Oversight Board.

17. CCTV Register

A CCTV Register shall be maintained by the Council's Data Protection Officer with the support of the Head of Digital Strategy. This register shall contain the following information:

- Location and GPS coordinates of each CCTV system (DPIA Grouping)
- Make and model of each CCTV system
- Purpose of each CCTV system
- CCTV service provider details
- Signage (GPS coordinates and map)
- 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
- Status of monitoring (live monitoring)
- Masking status

18. 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 of request;
- Date and time images were removed from the system (Monitoring Centre supervisors and Council designated staff members to keep a log);
- Location of footage, if appropriate (camera reference/location, (Monitoring Centre supervisors and Council designated staff members to keep a log);
- Description/reason for request, include An Garda Síochána pulse incident number;
- Date acknowledged by Data Protection Unit;
- Date section to respond and deadline (data subject access request only);
- Search and review completed by - include third party/processor/staff name;
- Signature confirmation from both collecting official and official providing CCTV footage (signing log book or confirmation letter);
- The extent of information to which access was allowed or which was disclosed;
- The outcome, if any, of the viewing or download e.g. not of evidential value;
- The date the images were deleted/ retained:
    - deleted: if not required by An Garda Síochána;
    - retained: on foot of a data subject access request in line with the National Retention Policy;
- The location of the data images, if retained.

19. 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. 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 the Council will be required to sign a Data Processing Agreement (DPA).

20. Data Subjects' Rights

Where CCTV recordings contain images of you, these images are your personal data and you have the following statutory rights in relation to this data which can be exercised at any time:

a) Right to information
b) Right to complain to supervisory authority
c) Right of access
d) Right to rectification or erasure
e) Right to be forgotten
f) Right to restrict processing
g) Right to data portability; and
h) Right to object and automated decision making/profiling

For further information, please see our Data Protection Policy available at https://www.limerick.ie/council/services/your-council/digital-services/cctv-creating-safer-communities or alternatively contact our Data Protection Officer at the contact details listed below.

Third country/international transfers

We do not transfer your personal data to a third country or international organisation. If, in the course of providing services to the Council, a third-party data processor should transfer data outside of the EEA, they may only do where there are appropriate safeguards in place to protect personal data and must ensure the provisions of Chapter V of the General Data Protection Regulation (GDPR) are complied with.

Automated decision making/profiling

We do not engage in automated decision-making/profiling.

21. Complaints to the Data Protection Commissioner

- Data subjects have the right to make a complaint at any time to the Data Protection Commission, the Irish supervisory authority for data protection issues.

Contact details for the Data Protection Commission are as follows:

- Go to their website www.dataprotection.ie
- Phone on +353 57 8684800 or +353 (0)761 104 800
- Email info@dataprotection.ie
- Address: Data Protection Office - Canal House, Station Road, Portarlington, Co. Laois, R32 AP23 or, alternatively 21 Fitzwilliam Square Dublin 2. D02 RD28 Ireland.

22. Contact Details of the Data Controller and the Data Protection Officer

Contact details of the Data Controller:

Limerick City and County Council

Address: Limerick City and County Council, Merchant's Quay, Limerick V94 EH90

Telephone: +353 61 556000

Email: customerservices@limerick.ie

Contact details for the Council's Data Protection Officer:

Dorothy Quinn - Data Protection Officer

Address: Limerick City and County Council, Merchant's Quay, Limerick V94 EH90

Telephone: +353 61 556000

Email: dataprotectionofficer@limerick.ie

Appendices

Appendix I – 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 in accordance with the terms of this policy and take account of the checklist issued in May 2019 by the Data Protection Commissioner.

DPC 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 Protection 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.

The DPC CCTV checklist should be considered in advance of proposing the installation of CCTV and provides guidance as to some of the key data protection considerations to be taken into account. The considerations outlined above are not exhaustive. For Community CCTV Schemes, please refer to An Garda Síochána code of practice for Community based CCTV Systems. Liaise with the Data Protection Officer and Head of Digital Strategy prior to undertaking any of the above.

Appendix II – Data Subject Access Request form

Comhairle Cathrach & Contae Luimnigh
Limerick City & County Council

Limerick City and County Council

Request for access to Personal Data (this includes CCTV and other Surveillance Technologies)

under the Data Protection Act 2018 and under Article 15 of the General Data Protection Regulation 2016

Name of Requestor: _____

Address: _____
(include eircode)

_____

_____

_____

Telephone No: _____

Email address: _____

*(We may need to contact you to discuss your access request)

Where a data subject makes a request, the information shall be provided by electronic means (email) where possible, unless otherwise requested by the data subject.

My preferred form of access is to receive records: (Please tick as appropriate)

- As above ☐
- by post ☐
- collect from Customer Services ☐

Details of Request:

I ……..wish to make an access request under Article 15 of the General Data Protection Regulation (GDPR) for a copy of any information Limerick City and County Council keep about me, on computer or in manual form in relation to the following:

When requesting information, it is important to give any details that will help the person to identify you and find your data – for example a staff number, date of birth, name of service(s) / section(s) and any account / case or reference number relevant to your access request along with any previous addresses that may assist.

Be clear about which details you are looking for if you only want certain information. This will help the Council to respond more efficiently. - see pages 4/5 of this document also.

If requesting access to CCTV & other Surveillance Technologies, please state the following:

Details of footage required:

Date:

Time: From: To:

Location:

Note 1: If you are seeking access to your own personal records, you may be required to provide photographic proof of identity. This is to make sure that personal information is not given to the wrong person.

Note 2: To process a CCTV or other Surveillance Technologies request, it will be necessary for the requestor to submit their own photographic ID in order to ensure that it matches with that on the recordings.

Note 3: If your request includes details of another individual (18 years or over), this information will be redacted. However, should you wish for this request to be treated as a joint request you will need to provide the written consent of that person.

Data Subject Declaration:

I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that Limerick City and County Council is obliged to confirm proof of identity/authority and it may be necessary to obtain further information to enable the Council to comply with this subject access request.

Print Name: _____

Signature: _____

Date: _____

Return to: Data Protection Officer
Limerick City and County Council
Merchants Quay
Limerick
V94 EH90

Email: dataprotectionofficer@limerick.ie
Tel: 061 556000

Right to make a complaint

If a data subject is not satisfied with our response, or if you do not receive a response, at that point you could make a formal complaint to the Data Protection Commission whose contact details are as follows:

Go to their website www.dataprotection.ie

- Phone on +353 57 8684800 or +353 (0)761 104 800
- Email info@dataprotection.ie
- Address: Data Protection Office - Canal House, Station Road, Portarlington, Co. Laois, R32 AP23. Or 21 Fitzwilliam Square Dublin 2. D02 RD28 Ireland.

Privacy Statement

Limerick City and County Council processes all personal information in accordance with the General Data Protection Regulation 2016 and the Data Protection Acts, 1988 to 2018.
The personal information (data) collected on this form is collected for the purpose of processing this application and any data collected is subject to Limerick City and County Councils privacy statement which can be found at – **https://www.limerick.ie/privacy-statement**

Comhairle Cathrach & Contae Luimnigh
Limerick City & County Council

Limerick City & County Council Departments

Department	Section	Please tick what section(s) you believe may hold records relating to your request	Dates (approx.) records relate to
Housing	Housing Application		
	Housing Rents		
	Tenant Purchase		
	HAP		
	RAS		
	Housing Maintenance		
	Other (please specify)		
Planning	Planning Application		
	Planning Enforcement		
	Other (please specify)		
Environment	Litter/Waste Management		
	Environmental Control		
	Burial Grounds		
	Other (please specify)		
Support Services	Corporate Services		
	Customer Services		
	Human Resources		
	Finance Services		
	Marketing & Communications		
	Other (please specify)		
National & Regional Shared Services	Fire & Emergency Services		
	Water Services		
	HAP Shared Service Centre		
	Southern Region Waste Management Office		
Economic Development	Strategic & Forward Planning		
	Trade & Investment		

Department	Section	Please tick what section(s) you believe may hold records relating to your request	Dates (approx.) records relate to
	Limerick Enterprise Office		
	Digital Services		
	Other (please specify)		
Community Development	Urban & Rural Community Development		
	Libraries Galleries & Museum		
	Tourism		
	Property & Community Facilities		
	Arts Office		
	Other (please specify)		
Travel & Transportation	Roads, Traffic, Cleansing		
	Travel & Transportation Strategy		
	Mid-West Road Design		
	Active Travel		
	Other (please specify)		

Appendix III – Download Request form

Comhairle Cathrach & Contae Luimnigh

Limerick City & County Council

Seirbhísí Corparáideacha,
Comhairle Cathrach agus Contae Luimnigh, Ceanncheathrú Chorparáideach,
Cé na gCeannaithe,
Luimneach

Corporate Services,
Limerick City and County Council,
Corporate Headquarters,
Merchants Quay,
Limerick

EIRCODE V94 EH90

t: +353 (0) 61 557150
f: +353 (0) 61 415266

Download Request Form

Date:
File Ref. No:

CCTV Download Request
[*Legislation Name*]

ATTN: [*Data Protection Officer*]

I wish to request approval to download CCTV footage required by Limerick City and County Council under the above legislation.

Please include the following:

Details of footage required:
Date:
Time: **From:** **To:**
Location:

Yours sincerely,

_____

(CCTV Officer)

APPROVED BY:

_____

(Data Protection Officer)

Date: _____