Comhairle Chontae na Gaillimhe
Galway County Council

CLOSED CIRCUIT TELEVISION POLICY

Introduction.

The following policy relates to surveillance camera equipment (CCTV), and the gathering, use, storage and disposal of CCTV system recorded data by Galway County Council. This includes CCTV systems within Council premises, car parks, piers, plant, civic amenity and locations in the ownership of Galway County Council, and includes the use of body worn video camera equipment. The CCTV systems are subject to legislation and Galway County Council undertakes to ensure that those who operate CCTV on its behalf do so within the terms of this policy to ensure continuing compliance with the following legislation-

Data Protection Acts (1988, 2003 and 2018),
The General Data Protection Regulations (EU) 2016/679,
The Freedom of Information Acts, Human Rights Act 1998,
Section 38 of the Garda Síochána Act, 2005.
Private Security Services Act 2004.
Safety Health and Welfare at Work Act 2005

1. Personal Data.

All CCTV and associated equipment are required to be compliant with this policy. Recognisable images captured by CCTV systems are “personal data” and subject to the provisions of the Data Protection Acts 1988- 2003 and 2018.

This policy document addresses these issues and sets out clearly what Galway County Council, as Data Controller, must do to protect personal data in relation to CCTV, while carrying out its statutory and other functions. This policy aims to set out standards relating to the use of such equipment that maximises effectiveness whilst at the same time minimises interference with the privacy of individuals whose images are captured by the devices.

2. Justification for Use of CCTV.

The Data Protection Act 1988 to 2018 requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that Galway County Council needs to be able to justify the obtaining and use of personal data by means of a CCTV system.

In addition to the obligations under the Data Protection Acts, the Human Rights Act 1998 requires any public authority using CCTV cameras to do so compatibly with Article 8 of the convention, and to assist in compliance with the Safety Health and Welfare at Work Act 2005.

Reasons for using CCTV.

3. Each CCTV system will have its own site or task specific objectives. These could include some or all of the following:

- Protecting areas and premises used by council officials and the public.
- Deterring and detecting crime and anti-social behaviour.
- Assisting in the identification of and apprehension of offenders in relation to public order offences.
- Deterring violent or aggressive behaviour towards council officials.
- Identifying those who have contravened parking regulations.
- Protecting council property and facilities.
- The occasional use of CCTV for covert monitoring of littler black spots
- To assist in the processing of allegations/claims against the Council.
- Monitoring Civic Amenity sites and Landfills
- Such other purposes as may arise from time to time.

The use of CCTV will be conducted in a professional, ethical and legal manner within the terms of this policy and the law. CCTV usage will be proportionate and CCTV systems will not be used to routinely monitor the activities of council employees or members of the public in the ordinary course of their lawful business.
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 so as 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

4. Video and Audio Recordings.

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

5. General Principles.

In terms of Community CCTV, while the Council has no role in law enforcement, it has provided CCTV in public places in order to facilitate the deterrence, prevention, detection and prosecution of offences as well as enhancing public safety and security. Section 38(3) of the Garda Síochána Act 2005 provides for the installation of CCTV systems for public security purposes under the authority of the Garda Commissioner.
Data obtained by CCTV may only be released when authorised by Personnel 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.

Covert Surveillance.

Galway 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. Covert surveillance is normally only permitted on a case by case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies an actual involvement of An Garda Síochána or an intention to involve An Garda Síochána.
Covert surveillance must be focused and of short duration. Only specific (and relevant) individuals/locations should be recorded. If no evidence is obtained within a reasonable period, the surveillance should cease.
Where An Garda Síochána requests to carry out covert surveillance in Council property,any request will be in writing.

6. Notification & Signage.

The Council will place this policy on its Intranet for the information and adherence of staff and on its website www.galway.ie for the information of the public.
All areas where CCTV is in use should be clearly signed. Such signs warn people that they are about to enter an area covered by a CCTV system or to remind them that they are still in an area covered by a CCTV system. Signs will also act as an additional deterrent.
Signs should :

- Be clearly visible and readable;
- Contain details of the organisation operating the system;
- The purpose for using the surveillance system;
- Contact details such as a simple website address, telephone number or email address.

WARNING
CCTV Cameras in Operation.

Images are being monitored and recorded for the purpose of crime-prevention, public safety, and for the protection of Galway County Council property.
This system is in operation 24 hours a day, it is controlled by Galway County Council and images may be passed to An Garda Síochána. For more information please ring 091 509000 or www.galway.ie

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

7. Storage & Retention.

Section 2(1)(c)(iv) of the Data Protection Act 1988 states that data ***"shall not be kept for longer than is necessary for the purposes for which it was obtained".*** This policy provides for a retention period of 28 days, except where the images identify an issue – such as a break-in or theft where such images / recordings are retained in relation to such events.
The recordings, DVRs, DVDs', servers etc. will be stored for the agreed retention period, then overwritten, and a log of access kept. CCTV access will be restricted to the designated staff member (Grade 7 or equivalent). Supervising the access, maintenance and security of the CCTV System is the responsibility of the relevant Director of Services who may delegate the administration of the CCTV System to other staff members. All images remain the property and copyright of the Council.

8. Access , Viewing Images and Disclosure to Third Parties.

Unauthorised access to recordings, monitors etc. will not be permitted at any time. Viewings must be carried out for a specific legitimate purpose. A log of access to monitoring stations and DVRs',

servers, DVDs' etc. will be maintained. Access where feasible will be password protected to limit unauthorised use.

In relevant circumstances, CCTV footage can be accessed (and a copy released subject to the relevant application being made)

- 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
- released to other statutory bodies as deemed appropriate; or
- to assist the relevant Director in establishing facts in alleged cases of unacceptable behaviour;
- 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
- released to individuals (or their legal representatives) subject to a Court Order.
- to the Council's insurers where it requires same in order to pursue a claim for damage done to the Council's insured property.

9. Access Requests by Data Subject.

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.

To exercise a right of access, a data subject must make an application in writing or by e-mail to the Data Protection Officer, Aras an Chontae, Prospect Hill, Galway. Or e-mail to dpo@galwaycoco.ie

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

In such circumstances it is good practice to put a hold on the deletion of the information, particularly where there is a set retention period which will mean that the information will be routinely deleted after a specified period.

Freedom of Information Acts

Under the Freedom of Information Acts, people can request access to any recorded information (with certain exemptions) that the council holds. However, if individuals are capable of being identified from the CCTV system footage then it is personal information about the individual concerned and is unlikely to be disclosed in response to a freedom of information request. A public authority who has surveillance systems, may also receive requests for information under FOIA relating to those surveillance systems. For example, requestors may ask for information regarding the operation of the systems, the siting of them, or the costs of using and maintaining them. If this information is held, then consideration will need to be given to whether or not it is appropriate to disclose this information under FOIA.

Requests under the FOI Acts should be addressed to: FOI Department, Corporate Services, Galway County Council, Prospect Hill, Galway.

10. CCTV in Meeting Rooms, Public Counters, Video and Audio Recording.

The Council provides a number of meeting rooms with CCTV. Customers, when seeking a meeting should be advised that such meetings will be held in a meeting room with a CCTV system and that it will be video and voice recorded. These rooms will display signs similar to that as shown in 6 above.

Customers objecting to such recording will not be met unless another member of staff is at the meeting as a witness, who will take notes and confirm with the customer the notes before the meeting concludes.

11. Audio Recordings.

The Council may provide audio recording systems in meeting rooms or on staff directly, in conjunction with CCTV in order 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, similar to that of video recordings in compliance with Section 7 above.

12. Responsibilities.

The relevant Director of Services has responsibility to-

- Ensure that the use of CCTV is implemented in accordance with the policy set down by Galway County Council,
- Oversee and co-ordinate the use of CCTV for safety and security purposes within Galway County Council,

- Ensure that all existing CCTV are evaluated for compliance with this policy,
- Ensure that the CCTV monitoring by the Council is consistent with the highest standards and protections,
- Review camera locations and be responsible for the release of any information or recorded CCTV material stored in compliance with this policy,
- Maintain a record of access (i.e. an access log) to, or the release of tapes or any material recorded or stored in the system,
- Ensure that no copies of recorded tapes are made without authorisation,
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally,
- 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 covert CCTV equipment or hidden surveillance cameras used for authorised criminal investigations by An Garda Síochána as approved by the County Secretary.]
- Give consideration to staff feedback / complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure 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,
- 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 DVRs’, DVDs’ etc. are stored in a secure place with access by authorised personnel only,
- Ensure that images recorded on DVRs’/DVDs/digital recordings are stored for a period 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 County Secretary,
- Ensure that when using a zoom facility on a camera, no invasion of privacy takes place and that such activity is logged.

13. Responsibility of Security Companies.

Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors". The Council will have a written contract-“Processor Agreement” with the Contractor /Security Company.

As Data Processors, they operate under the instruction of Data Controllers (Galway County Council). Sections 2(2) and 2C of the Data Protection Acts place a number of obligations on Data Processors.

These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all unlawful forms of

processing. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted.
Staff of the security company must be made aware of their obligations relating to the security of data.
Clients of the security company should have a contract in place which details what the security company may do with the data; what security standards should be in place and what verification procedures may apply.
Furthermore, section 16 of the Data Protection Acts 1988 & 2003(as amended) requires that all data processors must have an entry in the public register maintained by the Data Protection Commissioner, Those parties who are required to be registered and process data whilst not registered are committing a criminal offence and may face prosecution.
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.

14.Surveillance Technologies other than CCTV:

The Council Fires Service uses drones to get a visual of both bog and building fires.
The Council also uses drones to gather information for flood maps and flood risk situations, emergency response, Fire and Rescue, Severe Weather, Roads and Infrastructure development.
The Council has GPS tracking on our Gritting Machines only- as they work unsociable hours in bad weather.
The Council does not currently use dash cams on its vehicles.
The Council has ANPR cameras in 2 Estates in Tuam and this footage is covered under the provisions of this policy, with similar restrictions to access as the Housing Estate CCTV.
The Community Wardens may use their cameras to record parking infringements – as their hand held devices do not support this technology. These photos are deleted after the fine is paid, and only held as evidence, if Court action is pending.

IMPLEMENTATION AND REVIEW:

This code of practice will be reviewed and evaluated of foot of changing legislation or guidelines- from the Data Commissioner, and Garda Síochána, Internal or External Audit recommendations.
These reviews will ensure that legal requirements, policies and standards are complied with in practice.

This policy will apply from the date of adoption by Galway County Council Senior Management Team.

Policy and Procedure for the use of Body- Worn CCTV

Introduction:

This document sets out the Council's Policy and procedure for the use of Body Worn Cameras. Front line staff including but not restricted to: Community Wardens, Dog Wardens, and Housing Estate Management Staff may use these cameras. Currently Galway County Council is at Pilot stage in this regard and has only one BWC in use, with one further camera on order for a Community Warden. Eventually it is envisaged to have 15 BWCs in use.

BWV involves the use cameras that are worn by a person and are usually attached to their clothing or uniform. These devices can often record both visual and audio information.
BWV systems are likely to be more intrusive than the more 'normal' CCTV style surveillance systems because of its mobility.
The Council considers the use of BWV to be an appropriate measure to help protect the personal safety of the categories of frontline staff covered by this policy. Body Worn CCTV forms part of a Wardens Personal Protective Equipment and is provided solely for health and safety purposes, and to attain evidence of threatening or abusive behaviour against the employee.
Body Worn Cameras will not be used to gather evidence for Parking Enforcement or any other enforcement purposes.
Body worn CCTV will only be activated in the event where staff find themselves in a confrontational situation where they are subject to, or feel that they are likely to be subject to, verbal or physical abuse.

1. Recordings will not commence until the warden has issued a verbal announcement, where possible, of their intention to turn on the body worn device.
2. Recordings will not be made whilst performing normal patrolling duties.
3. All recordings will be held securely.
4. Access to recordings will be restricted to authorised personnel in the team and Senior Managers responsible.

Operational Procedures:

All Wardens will receive full training in the use of body worn CCTV. This training will include practical use of equipment, on street operational guidance and best practice, when to commence and cease recording and the legal implications of using such equipment.
Additionally, Wardens receive periodic refresher training in Conflict Awareness.
Individuals using BWV systems should be able to provide sufficient fair processing to data subjects. It is therefore important that clear signage is displayed, for example on an individual's uniform, to show that recording is taking place and whether the recording includes audio.
If the data subject wishes to find out more information, they can be directed to the Privacy notice, Policy document and our Subject Access Request policy on our website.

All recorded footage will be uploaded to the Council's I.T. system by the Line Manager. The Line Manager will ensure that any footage to be retained has been correctly bookmarked and that supporting Incident Reports have been completed.
For Incidents where An Garda Síochána have not been in attendance, the authorised staff member will review the recording and in consultation with the warden operating the device a decision will be made on whether referral to the Garda is appropriate.

The person responsible for the CCTV review will then transfer the data from the IT system on to a secure encrypted external hard drive and complete the Information Asset Log.
All retained data will be kept until all investigations have been completed or a prosecution has taken place.
Any other data not required for evidential purposes will be deleted by the person responsible for the CCTV Review by the next working day, Monday to Friday

The authorisation of staff to use a body worn camera requires a Chief Executive's Order.

Legislation:
The integrity of any video recording will be considered in accordance with the following legislation:
The Data protection Acts 1988, 2003(as amended), and 2018.
Freedom of Information Act 2015
Human Rights Act 1998- Article 6.
Safety health and Welfare Work Act 2005.

Data Access Request-
All data not required for evidential purposes will be deleted. However the GDPR regulations 2016, and S 91 of the Data Protection Act 2018, give individuals the right to access what information we hold on them and be given a copy of same. Any application to view footage is covered by Galway County Councils Data Protection Policy. Requests must be made in writing and suitable identification supplied to support the request.

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.

The date from which the policy will apply is the date of adoption by the Management of Galway County Council with implementation of and adherence to the policy to be monitored by the relevant Director of Services.

ends.

APPENDIX 1 of 1 – 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. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data.

Data Protection Acts – The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. The Council must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation

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.

ends.