CLARE COUNTY COUNCIL

CCTV AND OTHER SURVEILLANCE TECHNOLOGIES

POLICY

DP-POL-06

COMHAIRLE CONTAE AN CHLÁIR | CLARE COUNTY COUNCIL

REVISION HISTORY

DOCUMENT NO.	REVISION NO.	DETAILS	EFFECTIVE DATE	ISSUED BY:	APPROVED BY:
DP-POL-06	1	Initial development of a controlled document	**11/11/19**	**DPO**	**Management Team**
DP-POL-06	2	Updated to reflect DPC decisions on the use of surveillance technology by local authorities for certain enforcement functions	**17/05/21**	**a/DPO**	**Management Team**

Clare County Council
CCTV AND OTHER SURVEILLANCE TECHNOLOGIES POLICY

Contents

1. DEFINITIONS

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

"**ANPR"** automatic number plate recognition (see "**Surveillance systems**" below)

"**CCTV**": means Closed Circuit Television Systems which are fixed and domed cameras designed to capture and record images of individuals and property.

"**County Council**": means Clare County Council.

"**Data**": is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV and other surveillance systems, this generally means video images. It may also include static pictures such as printed screen shots.

"**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 is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

"**Data Protection Legislation**" means all applicable laws and regulations relating to the processing of personal data and privacy including the Data Protection Act 2018, the General Data Protection Regulation 2016/679 (the "**GDPR**") and any statutory instrument, order, rule or regulation made thereunder, as from time to time amended, extended, re-enacted or consolidated.

"**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 of our 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.

"**Smart CCTV":** means CCTV systems with the capacity for the images to be accessed remotely and in real-time.

"**Surveillance systems**": means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition ("**ANPR"**), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

2. EXECUTIVE SUMMARY

2.1 CCTV and other surveillance systems are installed in the offices, properties, depots, plant, and other locations in the ownership of the County Council or in the public spaces such as town centres, civic amenities, housing estates, halting sites, road junctions, etc.

2.2 CCTV technologies and other surveillance systems are a key component for securing public order and safety in public places by preventing, detecting or investigating offences or apprehending and prosecuting offenders and giving the residents a sense of safety. On the one hand, public safety can be supported by adequate CCTV technologies and other surveillance systems however on the other hand the systematic use of technologies can undermine individual privacy needs. This CCTV Policy is intended to address such concerns.

2.3 This document presents CCTV Policy for the County Council to cover the use of CCTV and other surveillance systems in County Council buildings & properties and also CCTV and other surveillance systems in public spaces.

2.4 We are committed to complying with our legal obligations and ensuring that the legal rights of individuals relating to their personal data are recognised and respected.

3. INTRODUCTION

3.1 For a free, unrestricted and unworried life people need to feel safe. In this context, having "eyes on the ground" in order to deter and reduce crime and offences, to better understand and respond to emergencies and to create safer communities is a key challenge for the County Council. Many communities have requested over the years the installation or an increase in the presence of CCTV for a better response to local concerns in relation to public order and safety in public places, dealing with offences and increasing the overall community safety.

3.2 To the extent that you are carrying out recording or surveillance in connection with civil defence, please review the Civil Defence CCTV Policy for guidance i.e. Small Unmanned Aircraft Ground School 2018, Civil Defence Branch, Department of Defence
Small Unmanned Aircraft (SAU) use is increasing rapidly and includes public service providers such as fire service, law enforcement, search and rescue and private and commercial operators. SAU includes drones.

4. PRIVACY AND DATA PROTECTION

4.1 CCTV technologies and other surveillance systems are a key component of preventing or detecting crime and giving the residents a sense of safety. On the one hand, safety perceptions can be supported by adequate CCTV technologies and other surveillance systems (e.g., smart cameras), however on the other hand, the systematic use of these technologies can undermine individual privacy needs.

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

4.3 Privacy and personal data protection is paramount. The CCTV Policy is defined having privacy, data protection and information security at its core. Video recording, processing and monitoring together with any data generated will be strictly controlled and governed under the relevant legislation and in particular the Garda Síochána Act 2005 and the Data Protection Act 2018 (including Part 5 of the Data Protection Act 2018 which implements the Law Enforcement Directive (EU) 2016/680 into Irish law) and also under the requirements of the GDPR. The County Council will also always seek to comply with best practice suggestions and guidance from the Data Protection Commission.

4.4 The County Council undertakes to operate its CCTV and other surveillance systems, and undertakes to ensure that those who operate CCTV and other surveillance systems on its behalf do so within the terms of this policy and the law and will review it regularly to ensure continuing compliance with the relevant legislation.

4.5 This policy document addresses these issues and sets out clearly what the County Council, as data controller, must do to protect personal data in relation to CCTV and other surveillance systems.

4.6 Before implementing new CCTV systems or other surveillance systems or before implementing changes to existing CCTV systems or other surveillance systems it may be necessary to conduct a Data Protection Impact Assessment ("**DPIA**"). An organisation must carry out a DPIA where proposed data processing "is likely to result in a high risk to the rights and freedoms of natural persons." The County Council's General Data Protection Policy contains further information on DPIAs and further information is also available on the Data Protection Commission website at www.dataprotection.ie.

5. PRIVATE AND PUBLIC CCTV SYSTEMS

5.1 The Council operates two types of CCTV systems:

5.1.1 Private CCTV systems and other surveillance systems; and

5.1.2 Public CCTV systems.

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

5.3 Public CCTV Systems operate in public places such as on streets, on roadways, bridges and other public places where the public have either an implied or express right of access.

5.4 This Policy distinguishes between private and public CCTV by noting that normally, for public CCTV, the consent of the Garda Commissioner is needed under Section 38(3) of the Garda Síochána Act 2005.

5.5 Regardless of whether CCTV and other surveillance systems are located in a private or public location, this Policy applies to these systems equally as do all the controls and standards as set out hereunder.

6. PURPOSE OF POLICY

6.1 This Policy relates to the use of CCTV systems and other surveillance systems, monitoring, recording, security, control, access and use of recorded material as well as setting out the way by which

6.1.1 Member of An Garda Siochana;

6.1.2 Council staff; and

6.1.3 Members of the public

can seek to access CCTV recordings and associated data.

6.2 The purpose of this Policy is to regulate the use of CCTV and its associated technologies and other surveillance systems and to ensure that such systems are operated in a manner compatible with this policy for:

6.2.1 Internal and external environs of premises under the remit of the County Council;

6.2.2 Public spaces;

6.2.3 The ongoing security of staff working alone or in handling law enforcement matters;

6.2.4 Data generated by Smart CCTV systems; and

6.2.5 Any other purposes as may arise from time to time.

7. CCTV SYSTEMS

7.1 CCTV and other surveillance systems are installed for the purpose of enhancing the safety and security of County Council premises, County Council staff and public spaces as well as creating awareness among buildings and public spaces users that security systems are in operation at all times, as detailed in the remaining part of this section. CCTV other surveillance systems are also installed 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.

7.1.1 Private CCTV Systems

Private CCTV Systems and other surveillance systems operate at premises such as County Council buildings, Fire Stations, Libraries, and other locations where the public do not have a right of access, be it implied or express (see Section 5) for the following purposes:

(a) Protecting the County Council's buildings and assets, both during and after office hours;

(b) Promoting the health, safety and welfare of staff, visitors and customers;

(c) Raising awareness for members of the public interacting with staff that their actions are being recorded in order to deter offences.

(d) It may also generally be a requirement of our insurer that such CCTV be in place

7.1.2 Public CCTV Systems

Public CCTV Systems operate in public places such as town centres, on streets, on roadways, bridges, at Bring Centres and other public places where the public have either an implied or express right of access (see Section 5 above)

The primary purpose for all CCTV and other surveillance systems is to secure public order and safety in public places including:

(a) 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;

(b) Improve emergency response e.g. accidents, fire, major emergency or severe weather incidents;

(c) Better traffic management and control, traffic counting and categorisation, traffic flow;

(d) Combat and reduce anti-social behaviour;

(e) Smart CCTV and ANPR (Automatic Number Plate Recognition) will also generate near real-time open statistical data such as traffic flows, pedestrian flows, line crossing, intrusion detection. All open data will be anonymised in an irreversible way before being accessed or used for any purpose and thus will not contain any personal data.

8. SMART CCTV AND DATA

8.1 This Policy covers CCTV and other surveillance systems that are capable of generating data.

8.2 For many years CCTV cameras were just that - simple standalone cameras that captured video of the area in front of them. However, the rapid technological advances occurring in the recent years provide new features, data capture and uses for CCTV, such as 360' view, traffic flows, pedestrian flows, line crossing, intrusion detection, etc. Also automatic recognition and artificial intelligence features such as ANPR and face recognition is now available in the more advanced CCTV systems and other surveillance systems. All these CCTV technological advances provide new opportunities to improve public and community safety and perception of safety by the local communities by better facilitating the deterrence, prevention, detection and prosecution of offences, assisting in identifying, apprehending and prosecuting offenders.

8.3 Smart CCTV and ANPR will also generate near real-time open statistical data such as traffic flows, pedestrian flows, line crossing, and intrusion detection. All open data will be

anonymised in an irreversible way before being accessed or used for any purpose and thus will not contain any personal data.

9. VIDEO RECORDINGS

9.1 This Policy covers CCTV systems that are capable of video recording.

9.2 The County Council does not operate Public or Private CCTV Systems or other surveillance systems with audio recording capabilities.

10. GENERAL PRINCIPLES

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

10.2 The following principles will apply for the use of any CCTV system or other surveillance systems:

10.2.1 The use of CCTV and other surveillance systems will be conducted in a professional, ethical and legal manner within the terms of this policy and the law.

10.2.2 Use of a CCTV and other surveillance systems must be for a specified purpose and necessary to meet an identified pressing need.

10.2.3 The use of CCTV and other surveillance systems must take into account its effect on the privacy of individuals, with regular reviews.

10.2.4 CCTV and other surveillance systems will not be located in areas where County Council staff and the public would have a reasonable expectation of privacy.

10.2.5 CCTV and other surveillance systems will not be used for monitoring employee performance. Information obtained in violation of this Policy may not be used in any disciplinary proceeding against any employee of the Council.

10.2.6 In relation to Public CCTV Systems, while the County 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.

10.2.7 CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the County Council, including Equality & Diversity, Dignity at Work, 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 Protection Commission.

10.2.8 There must be transparency, including a published contact point for access to information and complaints.

10.2.9 There must be clear responsibility and accountability for all system activities.

10.2.10 Clear rules, policies and procedures must be in place.

10.2.11 No more than the required images or information should be stored.

10.2.12 Access to retained images and information should be restricted with clearly defined rules on who can gain access and for what purpose.

10.2.13 CCTV and other surveillance systems operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

10.2.14 Images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10.2.15 There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

10.2.16 Any reference databases should be accurate and kept up to date.

10.2.17 CCTV and other surveillance systems should be used in the most effective way to support public safety and law enforcement to evidential standard.

10.3 All County Council CCTV and other surveillance systems and associated equipment are required to be compliant with this Policy.

11. CCTV USE

11.1 Article 5(1)(c) of the GDPR requires that data is "adequate, relevant and limited to what is necessary" for the purpose for which it is collected. This means that the County Council needs to be able to justify the obtaining and use of personal data by means of a CCTV and other surveillance systems.

11.2 The use of CCTV and other surveillance systems to control the perimeter of County Council buildings and property for security purposes is deemed to be justified and can be used to capture images of intruders or of individuals damaging property or removing goods without authorisation.

11.3 In other areas of offices where CCTV and other surveillance systems has been installed, e.g. hallways, stairwells, locker areas, canteens etc., these are to prevent risk to security and / or health & safety of staff.

11.4 Where it has been advised that surveillance of staff should take place, careful and appropriate use of CCTV and other surveillance systems can help to reduce risks to the security, health and safety of such staff subject to the fact that such surveillance must be limited to what is necessary for these purposes and any proposed new surveillance of staff should not be introduced without first receiving legal advice.

11.5 The purpose of CCTV and other surveillance systems in the public areas of our buildings is to enhance security and health and safety for all users of the buildings.

11.6 Within meeting rooms CCTV and other surveillance systems are used to ensure the security and health and safety of staff when meeting and interviewing visitors and customers.

11.7 The use of CCTV and other surveillance systems in public spaces is to act as a deterrent against anti-social behaviour and to deter, combat and prosecute offences and to help reduce crime in city and towns areas and at specific locations.

12. CCTV LOCATIONS

12.1 The location of cameras is a key consideration. According to the General Principles (see Section 10) the use of CCTV and other surveillance systems to monitor areas where individuals would have a reasonable expectation of privacy will not be allowed. 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.

12.2 Public CCTV Locations

Cameras can only be deployed at locations following a strategic assessment that identifies a need for CCTV or ANPR at that location to detect, deter and disrupt criminality. Strategic assessment takes account of:

12.2.1 Serious, organised and major crime

12.2.2 Local crime

12.2.3 Community confidence and reassurance, crime prevention and reduction.

Where a need is identified the camera may only be deployed if it is assessed as being appropriate and proportionate in balancing the protection of the public with the rights and individual expectations of privacy.

In addition the following aspects are considered

12.2.4 Maximise CCTV usage in a justified, legal way.

12.2.5 Maximise CCTV field of view in order to minimise the number of cameras deployed. This will lead to reduction of installation and maintenance costs and reduction in the perception of mass surveillance and privacy invasion

12.2.6 Consider co-location with other services that can share power, connectivity and CCTV column (sensors, public wifi, small cell mobile networks, etc.)

12.2.7 Deployment in housing estates to be considered on a case by case basis, on a justified need

12.2.8 Minimise visual impact of CCTV and the feeling of privacy intrusion

12.2.9 Consider the health & safety of the CCTV maintenance crews

12.2.10 Avoid overhead power lines

12.2.11 Avoid locations where vegetation can impact on visibility

12.2.12 Consider lighting conditions, recommended LED public lighting

12.2.13 Consider proximity of utilities: power and communications infrastructure

12.2.14 Consider the proximity of the CCTV hub location and line of sight for radio connections

12.2.15 Avoid proliferation and clutter of street cabinets

12.2.16 On footpaths, avoid disrupting pedestrian traffic including wheelchair users, prams or push chairs

12.2.17 On road junctions avoid locations where large good vehicles or truck can strike the CCTV equipment

12.2.18 Special areas of conservation or heritage

12.2.19 National monuments

12.2.20 At major street junctions and near roundabouts

Taking account of privacy impacts, most cameras including ANPR are located on higher volume traffic routes and only in exceptional circumstances within residential areas.

13. PUBLIC CCTV INSTALLATION REQUESTS FOR COMMUNITY CCTV SCHEMES

13.1 The installation of Public CCTV will be made using the following 7 steps and at all times in accordance with the Code of Practice for Community Based CCTV Systems published by the Department of Justice and Equality and An Garda Siochana:

13.1.1 A justified need identified by:

(a) Local elected representatives

(b) Community-based not-for-profit registered organisation that is representative of the community e.g. local community council, residents association, area partnerships, community development projects, family resource centres, community enterprise and supported by a local elected representative

(c) An Garda Siochana and requested by a member not below the rank of Superintendent or Acting Superintendent of the district for which the CCTV is requested

(d) Local Authority and requested by an approved officer with delegated responsibility for the prevention, detection and investigation of offences and for the prosecution of offenders

13.1.2 Assessment from the local An Garda Siochana Crime Prevention Officer.

13.1.3 Assessment by the County Council, with the oversight of the DPO, having regards to this Policy, Data Protection Legislation and the Garda Síochána Act 2005.

13.1.4 Allocation of adequate capital funding for installation and annual funding for maintenance, communications and monitoring costs

13.1.5 Public Consultation with the local community where the CCTV will be installed

13.1.6 Approval of the Clare Joint Policing Committee

13.1.7 Approval from An Garda Siochana Commissioner

13.2 The processes are iterative, i.e. applications for CCTV installation will need to pass each step before continuing to the next.

13.3 Any changes to existing CCTV locations will need to follow the same process.

14. CCTV VIDEO MONITORING AND RECORDING

14.1 CCTV video monitoring and recording may include the following:

14.1.1 Protection of County Council buildings and property: the building's perimeters, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services, customer service areas and meeting rooms.

14.1.2 Monitoring of access control systems: monitor and record restricted access areas at entrances to buildings and other areas.

14.1.3 Verification of security alarms: intrusion alarms, exit door controls, external alarms.

14.1.4 Video patrol (use of mobile cctv) of public areas: parking areas, main entrance /exit gates, traffic control.

14.1.5 Criminal investigations (carried out by An Garda Siochana): robbery, burglary and theft surveillance.

14.1.6 Investigations carried out by other agencies, e.g. the Marine Casualty Investigation Board: marine, air and other investigations following incidents.

15. COVERT SURVEILLANCE

15.1 The 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 and other surveillance systems is not in place, subject to this policy and Data Protection Legislation.

15.2 The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. 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, and where the surveillance is performed for a short, specified duration.

15.3 The purpose, justification, procedure, measures and safeguards that will be implemented must be documented when using covert surveillance with the final objective being, an

actual involvement of An Garda Síochána or other prosecution authorities for potential criminal investigation or civil legal proceedings being issued, arising as a consequence of an alleged committal of a criminal offence(s).

16. CCTV IN COUNCIL MEETING ROOMS

16.1 The County Council may provide a number of meeting rooms with CCTV facilities and other surveillance systems. When these facilities are provided, customers, when seeking a meeting should be advised that such meetings will be held in a meeting room with a CCTV or other surveillance systems and that it will be video recorded. These rooms will display appropriate signage to indicate the use of CCTV and other surveillance systems. Customers objecting to such recording will not be met unless another member of staff is present at the meeting as a witness, who will take notes and confirm with the customer the notes before the meeting concludes.

16.2 The County Council may provide CCTV and other surveillance systems in meeting rooms or to staff directly, 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 video recorded.

17. SMART CCTV AND DATA

17.1 The rapid technological advances occurring in the recent years provide new “smart” features, data capture and uses for CCTV, such as 360' view, traffic flows, pedestrian flows, line crossing, intrusion detection, seismic or heat detection when cameras are subject to vandalism, etc. Also automatic recognition and artificial intelligence features such as ANPR and face recognition are now available in the more advanced CCTV systems. All these CCTV technological advances provide new opportunities to improve public and community safety and perception of safety by the local communities by better facilitating the deterrence, prevention, detection and prosecution of offences, assisting in identifying, apprehending and prosecuting offenders.

17.2 Smart CCTV and ANPR will also generate near real-time open statistical data such as traffic flows, pedestrian flows, line crossing, intrusion detection, etc. All open data will be anonymised in an irreversible way before being accessed or used for any purpose and thus will not contain any personal data.

18. ANONYMISATION AND PSEUDONYMISATION

E.g. For the purposes of access requests-Pixelation or other types of anonymisation carried out on cctv or other surveillance data/images/footage (usually has to be carried out by experts)

18.1 When carried out effectively, “anonymisation” and “pseudonymisation” can be used to protect the privacy rights of individual data subjects and allow organisations to balance this right to privacy against their legitimate goals.

18.2 "Anonymisation" of data means processing it with the aim of irreversibly preventing the identification of the individual to whom it relates. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.

18.3 "Pseudonymisation" of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified.

18.4 Although pseudonymisation has many uses, it should be distinguished from anonymisation, as it only provides a limited protection for the identity of data subjects in many cases as it still allows identification using indirect means. Where a pseudonym is used, it is often possible to identify the data subject by analysing the underlying or related data.

18.5 Irreversibly and effectively anonymised data is not “personal data” and the data protection principles do not have to be complied with in respect of such data. Pseudonymised data remains personal data.

18.6 If the source data is not deleted at the same time that the anonymised data is prepared, the anonymised data will still be considered “personal data”, subject to the Data Protection Legislation, where the source data could be used to identify an individual from the anonymised data.

18.7 Data can be considered “anonymised” from a data protection perspective when data subjects are not identified, having regard to all methods reasonably likely to be used by the data controller or any other person to identify the data subject.

19. SMART CCTV AND ANPR DATA USAGE

19.1 Smart CCTV and ANPR generate near real-time open statistical data such as traffic flows, pedestrian flows, line crossing, intrusion detection, etc.

19.2 ANPR consists of a camera that is linked to a computer. When a vehicle passes by the camera the camera records an image which is automatically ‘read’ by the computer and the vehicle registration number recorded. ANPR technology is used to help detect, deter and disrupt criminality at a local, regional and national level, including tackling travelling criminals and organised crime groups.

19.3 It is accepted that ANPR data is ‘personal data’ within the meaning of the GDPR. A Vehicle Registration Number is not in itself ‘personal data’ however since local authorities can in most cases access data that links a person to the vehicle, for example the name of the registered keeper it is ‘personal data’ within the meaning of the GDPR. Personal data for vehicles can only be obtained if for example an offence has been committed and the registered keeper can be required to provide details of the driver.

19.4 The record for all vehicles passing by a camera, including those vehicles that are not known to be of interest at the time of the ANPR read may in appropriate circumstances be accessed for investigative purposes. The use of ANPR in this way has proved to be

important in the detection of many offences, including locating stolen vehicles, tackling uninsured vehicle use and solving cases of major and organised crime.

19.5 All open data will be anonymised in an irreversible way before being accessed or used for any purpose as follows:

19.5.1 ANPR data – will only be used retrospectively as a software solution to facilitate faster retrieval of relevant CCTV footage based on an An Garda Investigation request or a County Council investigation and only for the purpose of facilitating the deterrence, prevention, detection and prosecution of offences. There are no automatic links made between the vehicle registration number and the vehicle registration database or speed enforcement systems. Access to ANPR data may only be by authorised persons for investigation and intelligence purposes. These controls ensure that the majority of ANPR read records enter the system automatically as a vehicle passes by a camera and are then deleted from the system without ever being accessed in the interim period.

19.5.2 ANPR irreversibly anonymised data will be used for statistical purposes e.g. traffic flows, traffic volumes, traffic types, etc. and published as open data for the public.

19.5.3 pedestrian counting estimates footfall (the number of pedestrians) by accumulating low-level features foreground pixels and motion vectors on a virtual gate (virtual line). No personal identifiable data is being captured as part of this feature

19.5.4 Line crossing, intrusion detection and any other forms of detection are to detect if there is any object entering or leaving the area, it will trigger a rule, such as; when crossing the area perimeter, support enter, leave and enter and leave three direction selection, it can activate record, snapshot and alarm according to the judgement result.

20. NOTIFICATION & SIGNAGE

20.1 Adequate CCTV signage must immediately be placed at locations where CCTV camera(s) and other surveillance systems are installed, including at entrances to County Council offices and property as well as advance notices indicating the use of CCTV and other surveillance systems. Signage will include

20.1.1 The identity of the Data Controller

20.1.2 Contact details of the Council's Data Controller

20.1.3 The specific purpose(s) for which the CCTV camera or other surveillance systems is in place in each location.

20.1.4 Signs must also comply with the Official Languages Act and any other relevant legislation regarding sign standards.

20.2 Appropriate locations for signage include:

20.2.1 At or close to each camera

20.2.2 Entrances to premises, i.e. external doors and entrance gates

20.2.3 Reception areas

20.2.4 Any other areas covered by CCTV or other surveillance systems

20.3 As part of this policy the County Council will regularly advertise the fact that staff may use video recording devices during the course of their work. The staff members, when using CCTV equipment or other recording technologies, must advise persons approaching them that the interaction is being recorded by way of video.

20.4 The County Council will publish this policy on its Intranet for the information and adherence of staff and on its website [***insert hyperlink***] for public awareness and information.

21. CCTV RECORDING, STORAGE, RETENTION AND BREACH NOTIFICATIONS

21.1 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".

21.1.1 Private CCTV and other surveillance systems - a retention period of 28 days applies, unless there are specific, legitimate and reasonable grounds for the retention of images beyond that period. CCTV images should be erased and media storage devices re-used after a period of 28 days unless required for the investigation of offences or evidential purposes. Media storage devices that cannot be erased (e.g. single use CD/ DVDs) should be destroyed after a period of 28 days unless required for the investigation of offences or evidential purposes.

21.1.2 Public CCTV Systems - a retention period of 28 days applies, unless there are specific, legitimate and reasonable grounds for the retention of images beyond that period. CCTV images should be erased and media storage devices re-used after a period of 28 days unless required for the investigation of offences or evidential purposes. Media storage devices that cannot be erased (e.g. single use CD/ DVDs) should be destroyed after a period of 28 days unless required for the investigation of offences or evidential purposes.

21.1.3 ANPR data is considered CCTV data and the same retention period of 28 days applies.

21.2 Where footage has been identified that relates to a specific incident, a longer period may be justifiable for the particular section of footage concerned, such as in the investigation of a workplace accident or where footage may be used in criminal proceedings. This footage may be retained beyond the 28 day standard retention period in such circumstances. This footage should be isolated from the general recordings and kept securely for the purposes that have arisen. The decision to deviate from the 28 day retention period must be approved an Approved Officer and this decision, together with the reasoning for making that decision should be documented.

21.3 The recordings in any format (tapes, DVDs', servers, etc.) must be stored in secure environments.

21.4 An access log must be maintained and made available for inspection on request from Data Protection Officer or any designated officer.

21.5 At the end of their retention period, recordings and images will be erased permanently and securely. Any physical matter such as tapes, discs, photographs or hard copy prints will be disposed of as confidential waste.

21.6 Access will be restricted strictly to authorised personnel.

21.7 Supervising the access and maintenance of the CCTV and other surveillance systems is the responsibility of a representative of each department operating CCTV and other surveillance systems or other Approved Officer based on a written approval of the Director of Services, who may delegate the administration of the CCTV and other surveillance systems to other staff members.

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

21.9 If, in the operation of a CCTV and other surveillance systems, it becomes apparent that there may have been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the CCTV or surveillance system, the County Council's Data Breach Policy and Procedure must be consulted and complied with.

22. ACCESSING AND DOWNLOADING CCTV FOOTAGE

22.1 Unauthorised access to live CCTV or other surveillance systems, recordings, monitors etc. will not be permitted at any time.

22.2 Monitoring stations will be kept locked. A log of access to monitoring stations and tapes, servers, DVDs' etc. will be maintained.

22.3 In relevant circumstances, CCTV and other surveillance systems footage may be downloaded by:

22.3.1 Authorised Officers (see 22.3.2) of the council for An Garda Síochána Officers only when a formal written request is provided to the County Council and/or data processor stating that An Garda Síochána is investigating a criminal matter. For practical purposes, and to expedite a request speedily in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. However, any such verbal request must be followed up with a formal written request. A log of all An Garda Síochána requests must be maintained. Any such requests should be on An Garda Síochána headed paper, quote the details of the CCTV footage required and should also cite the legal basis for the request. With regard to Community CCTV these requests must be signed by a member of the Garda Síochána of a rank not lower that of Superintendent. Any such requests which are made directly to the data processor instead of the

County Council must result in a copy of the request being furnished to the County Council by the data processor; or

22.3.2 Authorised Officers – designated council staff as listed in APPENDIX A, on request in writing as described in the procedure detailed in APPENDIX B, using the form presented in APPENDIX C, only for the purpose of facilitating the deterrence, prevention, detection and prosecution of offences under the relevant legislation or for the purposes of the protection of health and safety, for the purposes of defending or bringing claims relating to health and safety or other related and pre-approved purposes. For practical purposes, and to expedite a request speedily in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. However, any such verbal request must be followed up with a formal written request no later than 5 days. A log of all designated council staff requests must be maintained. Any such requests should be on County Council headed paper, quote the 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 investigation is undertaken; or

22.3.3 Data subjects (or their legal representatives), pursuant to an access request under the Data Protection Legislation, where the time, date and location of the recordings is furnished to the County Council; or

22.3.4 Individuals (or their legal representatives) subject to a court order.

22.4 There is a distinction between a request by An Garda Síochána to view CCTV footage and to download copies of CCTV footage. In general, An Garda Síochána making a request to simply view footage on the premises of a data controller or processor would not raise any specific concerns from a data protection perspective however any such requests should nonetheless be logged.

23. ACCESS REQUESTS UNDER DATA PROTECTION LEGISLATION

23.1 Access to CCTV and other surveillance systems recording is facilitated and subject to the Data Protection Policy including the County Council General Data Protection Policy and the County Council Response Procedures for Data Subject Requests as for any other personal data access request. Under the Data Protection Legislation, on 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.

23.2 Where the image / recording identifies another individual, those images may be released where they can be redacted / anonymised so that other persons are not identified or identifiable. In circumstances where the data cannot be effectively anonymised, the controller shall not provide the data subject with the information that constitutes such personal data relating to the other individual, and shall provide the data subject with a summary of the personal data concerned that, in so far as possible, permits the data subject to exercise his or her rights and does not reveal, or is not capable of revealing the identity of the other individual.

23.3 To exercise a right of access, a data subject must make an application via the Data Protection Officer in the County Council, and a response may issue within one month (unless an extension of time is necessary, in which case such extension shall be notified to the data subject within one month together with reasons for extension).

23.4 To facilitate access requests the following will be necessary:

23.4.1 A person should provide all the necessary information to assist the Council in locating the CCTV and other surveillance systems recorded data, such as the location, date and time 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 therefore not subject to Data Protection Legislation covering access requests.

23.4.2 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 and other surveillance systems.

23.4.3 In giving a person a copy of their data, the County Council may provide a still/series of still pictures or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

23.4.4 For more information on making requests for personal data under the Data Protection Legislation please consult the County Council's *Privacy Statement] / [Appendix II of the County Council's Response Procedures for Data Subject Requests*]

24. ROLES AND RESPONSIBILITIES

24.1 The management team has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy.

24.2 Day-to-day management for deciding what information is recorded, how it will be used and to whom it may be disclosed shall be the responsibility of each Director of Service of the County Council which implements CCTV or other surveillance systems. An individual or team will be nominated in each department to assume responsibility for that department.

24.3 An individual or team will be nominated in each department to assume day-to-day operational responsibility for CCTV cameras and other surveillance systems and the storage of data recorded.

The main duties and responsibilities of the County Council are to:

24.3.1 Ensure that the use of CCTV and other surveillance systems is implemented in accordance with the policy set down by the County Council,

24.3.2 Oversee and co-ordinate the use of CCTV and other surveillance systems for safety and security purposes within the County Council,

24.3.3 Maintain the list of CCTV and other surveillance systems installation requests, internal and external, and makes recommendations for new camera installations in line with the CCTV strategy and CCTV Policy,

24.3.4 Maintain the Authorised CCTV Officers List as included in APPENDIX A,

24.3.5 Maintain the CCTV Access Procedure included in APPENDIX B,

24.3.6 Maintain the CCTV and other surveillance systems asset register,

24.3.7 Ensure that all existing CCTV and other surveillance systems are evaluated for compliance with this policy,

24.3.8 Ensure that the CCTV and other surveillance systems monitoring by the Council is consistent with the highest standards and protections,

24.3.9 Responsible for the release of any information or recorded CCTV and other surveillance systems material stored in compliance with this policy,

24.3.10 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,

24.3.11 Ensure that no copies of recordings are made without authorisation,

24.3.12 Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally,

24.3.13 Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. Temporary cameras do not include covert CCTV equipment or hidden surveillance cameras used for authorised criminal investigations by An Garda Síochána.

24.3.14 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.

24.3.15 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,

24.3.16 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",

24.3.17 Ensure that any storage media (DVDs, CDs, USB devices, etc.) are stored in a secure place with access by authorised personnel only

24.3.18 Ensure that images recorded 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.

25. MONITORING SERVICES

25.1 The CCTV and other surveillance systems if controlled by a security company contracted by the County Council will comply with this policy and the following:

25.1.1 The County Council will ensure that it only contracts security firms which are registered as either installers or monitors of CCTV and other surveillance systems under the Private Security Authority Act, 2004 as amended.

25.1.2 The County Council will have a written contract with the security company in place which details the areas to be monitored, how long data is to be stored, what the security company may do with the data, what security standards should be in place and what verification procedures apply.

25.1.3 The written contract will state that the organisation will give the County Council all reasonable assistance to deal with any data subject request made under Articles 15 – 22 of the GDPR which may be received by the Council to ensure the compliance, by the County Council, with the request within the statutory time-frame (generally 1 month).

25.2 Organisations providing CCTV and other surveillance systems monitoring services (e.g. community centres, security companies) that place and/or operate CCTV and other surveillance systems on behalf of the County Council are considered to be "data processors". As data processors, they operate under the instruction of data controllers. Article 28 of the GDPR stipulates that there must exist a contract between the controller and the processor. This contract must provide, in particular, that the processor shall:

25.2.1 Act only on instructions from the controller in relation to the processing, except in circumstances where the law of the European Union or the law of the State requires otherwise,

25.2.2 Procure the services of another processor only where authorised to do so in advance and in writing by the controller,

25.2.3 Ensure that any person authorised to process the personal data has undertaken to maintain the confidentiality of the personal data or is under an appropriate statutory obligation to do so,

25.2.4 Take all measures required by Article 32 of the GDPR,

25.2.5 Assist the controller in ensuring compliance in relation to the exercise by a data subject of his or her rights,

25.2.6 Erase or return to the controller, at the election of the controller, all personal data upon completion of the processing services, and erase any copy of the data unless required by law to retain the data,

25.2.7 Make available to the controller all information necessary to demonstrate compliance by the processor with the relevant legislation.

25.3 The County 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. Staff of the County Council must be made aware of their obligations relating to the security of data.

26. USE OF ADDITIONAL SURVEILLANCE SYSTEMS AND/OR CHANGES TO EXISTING SYSTEMS

26.1 Where a surveillance system uses new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the County Council shall, prior to the processing, carry out an assessment (a data protection impact assessment or "**DPIA**") of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar risks.

26.2 Prior to the introduction of any new surveillance system, or changes to an existing system, including placing a new CCTV camera or other surveillance equipment in any workplace location, we will carefully consider if they are appropriate by carrying out a DPIA.

26.3 A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

26.4 Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

27. DOCUMENT OWNER AND APPROVAL

27.1 The Data Protection Officer is responsible for ensuring that this Policy document is reviewed in line with the review requirements stated above.

27.2 The County Council reserves the right to change this Policy at any time without notice to County Council Personnel so please check back regularly to obtain the latest copy of this Policy.

27.3 A current version of this document is available on the Council intranet and extranets.

27.4 This Policy was approved by the Management Team and is issued on a version controlled basis.

27.5 This Policy does not override any applicable national data privacy laws and regulations in countries where the County Council operates.

28. APPENDIX A: CCTV AND OTHER SURVEILLANCE SYSTEMS ACCESS BY DOMAIN AND AUTHORISED OFFICERS

Version: 0.1

Last Modified: [/ /2019]

This section identifies the domains (areas or activities) for which CCTV and other surveillance systems will be utilised.

1. CHANGE LOG

Ver.	Date	Change log	Authors
0.1	/ /2019	Initial draft	

2. CCTV and other surveillance systems Use Domains

The primary purpose of Public CCTV use by the County Council is to improve 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.

Local Authorities have obligations under various legislation (Acts, statutory instruments, byelaws, etc) for prevention, detection, enforcement and prosecution of offences. A list of the legislation for which the County Council has such obligations is listed in the table below.

ID	Access Domain	Sub-domain	Legislation (as amended)
1	Emergency Response	Protection of People and Critical Infrastructure in case of: - Natural Disasters (flooding, - Technological Emergencies - Transport Accidents - Security	A Framework for Major Emergency Management. Local Co-ordination Group Principal Response Agencies (An Garda Síochána, HSE, local authorities)
2	Fire Safety	Fire Fighting	Fire Services Act
3	Anti-Social Behaviour	Anti-social Behaviour	Criminal Justice Act Housing (Miscellaneous Provisions) Act
4	Property Protection	Property Protection	Housing (Miscellaneous Provisions) Act Housing (Traveller Accommodation) Act Criminal Justice Act
5	Property Protection	Public Liability Claims,	Local Government Act, 2001

		Security purposes Protection of the public	Criminal Justice Act
6	Traffic Control	Traffic Control	Road Traffic Act Local Authorities (Traffic Wardens) Act
7	Environmental Control	Waste Control (Illegal Dumping)	Waste Management Act
8	Environmental Control	Burning of Waste	Air Pollution Act
9	Environmental Control	Litter Control	Litter Pollution Act
10	Environmental Control	Dog Control	Dog Litter & Dog Control Byelaws
12	Environmental Control	Horse Control	Control of Horses Bye-Laws
13	Environmental Control	Animal Control	Animal Health and Welfare Act
14	Environmental Control	Public Parks	Public Park Bye-Laws
15	Staff Safety	Staff Safety	Safety, Health and Welfare at Work Act
16	Control & Enforcement	Any	Any other legislation for which the Council has obligations as the prosecuting authority

3. Authorised Officers

The council has designated a number of Council staff who are authorised to access CCTV and other surveillance systems footage. All officers must be Garda vetted.

29. APPENDIX B: CCTV AND OTHER SURVEILLANCE SYSTEMS ACCESS PROCEDURE

The objective of this section is to standardise the method by which staff in the County Council can access CCTV and other surveillance systems footage in order to ensure compliance with privacy and data protection legislation including GDPR.

The primary purpose is to ensure that the appropriate control measures are in place and that all employees of the County Council with permissions to access CCTV and other surveillance systems footage follow this procedure. CCTV and other surveillance systems recordings can only be accessed by designated staff members as included in APPENDIX A as Authorised Officers.

Designated staff members must be Garda vetted before being placed on the CCTV Authorised Officers list.

Procedure for accessing CCTV and other surveillance systems footage

CCTV and other surveillance systems footage can only be accessed by Authorised Officers as included in APPENDIX A. The request to *view* CCTV and other surveillance systems footage requires no special permissions however the access must be logged in each department. Logs must be provided to the DPO upon request.

Procedure to download footage from the CCTV system

CCTV and other surveillance systems requests for download of footage from Council owned CCTV and other surveillance systems can be made:

- Only by Authorised Officers included in APPENDIX A and
- Only for the purpose of facilitating the deterrence, prevention, detection and prosecution of offences under the legislation, or
- Only for the purposes listed in this Policy as listed in Section 22.

To obtain a download from Council CCTV and other surveillance systems the Authorised Officer must:

1. Submit in writing a CCTV and other surveillance systems download request to the relevant Approved Officer. The Authorised Officer must have a formal Delegation Order from the Chief Executive with responsibility for facilitating the deterrence, prevention, detection and prosecution of offences under the legislation

2. The request must be based on a formal inspection process, include the unique CRM or other tracking method, inspection number, an explanation outlining the reason for seeking the download, the location, date and time for CCTV and other surveillance systems and also cite the legal basis for the request (The Act, Section, etc. under which the inspection is undertaken).

3. The Approved Officer must ensure that the request complies with: Data Protection Legislation, the underlying legislation under which the request is made and this CCTV and other surveillance systems Policy.

4. The Approved Officer will approve the CCTV and other surveillance systems Download Request and return this signed CCTV and other surveillance systems download request to the Authorised Officer only when satisfied that all the conditions have been met

5. The Authorised Officer must keep a copy of the approved CCTV and other surveillance systems download request in the inspection record and (where applicable) present the original approved CCTV and other surveillance systems request to the CCTV and other surveillance systems data processor in order to obtain the footage.

6. The CCTV and other surveillance systems processor 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 County Council of all CCTV and other surveillance systems download requests regardless of whether they are approved or not.

Each department of the County Council operating CCTV and other surveillance systems will report to the DPO on an annual basis:

- Total Number of CCTV and other surveillance systems download requests
- Number of CCTV and other surveillance systems download requests approved
- Number of CCTV and other surveillance systems download requests rejected

30. APPENDIX C: SAMPLE DOWNLOAD REQUEST FORM

CCTV AND OTHER SURVEILLANCE SYSTEMS

NB: *This is a request to download and view footage / images. If the footage is later to be used for another purpose or passed on to a third party, a new legal basis will have to be established and potentially a new agreement entered into.*

Date:
Download Request Number:
File Ref. No:

Name of department requesting access:

ATTENTION: [***Approved Officer***]

I wish to request approval to download of CCTV or other surveillance systems footage required for inspection.

Please indicate type of download:

☐ CCTV Download Request

☐ other surveillance systems –please specify type of system: _____

[***Download Request number***], [***Inspection Subject***] for:

[***Download Details***]

[***Legislation Name***]

under the above legislation from the following location:

[***Inspection Location***]

And for the following period

[***Date/Time***]
Yours sincerely,

_____
Authorised Officer

APPROVED BY:

_____ Date: _____
Approved Officer