South Dublin County Council CCTV Code of Practice

For the operation of Closed Circuit Television (CCTV) Systems for security or other purposes in Council owned or other premises under the remit of South Dublin County Council.

UPDATED - APRIL 2020

1. Code of Practice Statement

1.1. This Code of Practice details the operation and control of Closed Circuit Television (CCTV) Systems which are installed in a number of locations under the remit of South Dublin County Council.

1.2. The use of CCTV systems will be conducted in a professional, ethical and legal manner. Of primary concern is making sure that the privacy of individuals is protected in line with the General Data Protection Regulation and the Data Protection Acts 1988 to 2018. These Acts provide for the collection, processing, retention and eventual destruction of personal data in a responsible and secure way, thereby avoiding its misuse. For further information, see the Council's Data Protection Policy and Privacy Statement (available at https://www.sdcc.ie/en/services/our-council/access-to-information/data-protection/).

2. Scope

2.1. This Code of Practice applies to all personnel, property and other locations under the remit of South Dublin County Council and relates directly to the location and use of CCTV, the monitoring, recording and subsequent use of and access to such material. It also relates to any Community based CCTV Systems where South Dublin County Council has a data controller role.

3. Relevant Legislation and Corporate Policies

3.1. All CCTV Systems operated by or on behalf of South Dublin County Council must operate in compliance with:

- Data Protection Acts 1988 to 2018;
- General Data Protection Regulation
- Garda Síochána Act 2005;
- South Dublin County Council's CCTV Code of Practice, Data Protection Policy and Data Protection Compliance Guidelines;
- Private Security Authority Licensing requirements (Private Security Services Act, 2004).

4. CCTV Systems used by South Dublin County Council

4.1. There are currently three main types of CCTV systems in use by the Council. They are:

4.1.1. Council offices, works depots and libraries;

4.1.2. Dedicated Traffic Cameras at major junctions and on traffic routes throughout the county;

4.1.3. Public safety systems in residential and public realm areas for example, estate management, parks, playgrounds, recycling facilities.

4.2 Community facilities, such as the Civic Theatre, Rua Red, swimming pools, leisure and community centres, that are owned by the Council but managed by another entity must provide written confirmation that the operation and use of the CCTV systems within the premises and / or vicinity is in compliance with the General Data Protection Regulation(GDPR) and all current Irish Data Protection legislation.

4.3 There are a small number of Community based CCTV systems which are approved by An Garda Síochána which monitors the CCTV images for its law enforcement purposes.

4.4 The Grand Canal Green Route CCTV system is operated by Grangecastle Business Park on behalf of South Dublin County Council.

4.5 A web enabled centralised record management system serves as a comprehensive inventory of all South Dublin County Council CCTV Systems in operation with the objective of each detailed and Authorised Persons and their nominee(s) of each system clearly stated. Each department is responsible for updating the inventory for all systems under its control.

5. Purposes of CCTV

5.1. The purposes for which CCTV systems are installed include:

- To assist in providing for the security and safety of all visitors and staff;
- To monitor and protect Council buildings and facilities;
- To assist real-time monitoring and management of traffic conditions on the national and local road network throughout the county;
- To assist in emergency response situations for example, accidents, flooding, winter weather conditions and so on;
- To assist in the prevention and detection of crime;
- To facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order offences;
- To assist in the processing of allegations / claims against the Council;
- To assist the enforcement of Council car parking regulations and management of these car parks.

5.2. The use of CCTV is signalled by notices placed at entrances to and in prominent locations across the premises / in the vicinity of the cameras. Such notices must clearly identify the role of South Dublin County Council as data controller, identify the purpose for which the CCTV is being used and include a Council contact telephone number. CCTV which is monitored by An Garda Siochana must clearly indicate that such monitoring takes place in the notices provided.

5.3. Although every effort has been made in the layout of the CCTV systems to give them maximum effectiveness, it is not possible to guarantee that they will detect every incident that takes place in the vicinity.

6. Covert Surveillance

6.1 Covert surveillance is 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 or an intention to involve An Garda Síochána and any other prosecution authorities for potential criminal investigation or civil legal proceedings being issued, arising as a result of an alleged committal of a criminal offence.

6.2 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 stop.

6.3 If the surveillance is intended to prevent crime, overt cameras may be considered to be a more appropriate measure, and less invasive of individual privacy.

6.4 Permission of the Chief Executive (CE) must be obtained before considering covert surveillance.

7. Management of CCTV Footage

7.1. All recorded CCTV footage must be adequately secured and access to playback of recorded footage must be password-controlled. Sharing of passwords should never occur and each person authorised to access footage must have his/her own unique password.

7.2 The Traffic Management Centre Controller and his / her nominee(s) are responsible for the procurement, technical operation and maintenance of all systems that this code of practice applies to, as set out in section 4.1 other than those systems directly managed and monitored by individual departments which will be responsible for such systems. The systems will be procured, managed and maintained in accordance with

data protection legislation and for the purposes of the CCTV systems as set out in Section 5 of this code.

7.3 Each system must identify an Authorised Person within the Council and his / her nominee(s) who are authorised to operate and monitor that CCTV system. Details of the Authorised Persons and nominees must be recorded on the CCTV System Inventory and forwarded to the Traffic Management Centre Controller.

7.4 Access logs are to be maintained by the Authorised Person or his / her nominee(s) in accordance with data protection legislation. Access logs will be subject to periodic inspection by the Council's Data Protection Officer and Internal Audit Section and additionally in the event of audit by the Data Protection Commission. Each Authorised Person will be required to provide written confirmation to the Council's Data Protection Officer annually of the position in relation to maintenance of the access logs for the preceding year.

7.5 All Authorised Persons and nominees will be appointed by Chief Executive Order.

7.6 Authorised personnel are responsible for making sure that the system is only used in an appropriate manner in conformance with legislative requirements.

7.7 Authorised personnel must make sure that all nominees are fully briefed in respect of operational, administrative and legislative requirements that arise from the management of the CCTV system and recorded footage.

7.8 Recording by staff or appointed data processors of any CCTV images on mobile phones or other video recording devices is strictly prohibited.

8.Retention of CCTV Footage

8.1 Recorded footage on the CCTV system

8.1.1. In accordance with the Data Protection Acts, CCTV footage is retained for no longer than is necessary. In general, footage will only be retained for a period of 28 days unless valid reasons including those set out in section 5.1 above arise.

8.2 Footage from the CCTV system retained as evidence

8.2.1 The following log of retained recorded CCTV footage will be maintained by the named Authorised Persons or his / her nominee(s), as set out in Section 7:

- the date and nature of the matter recorded;
- the date(s) of when the CCTV footage was accessed and copied;
- record of any disclosure of CCTV footage;
- record of when and how the CCTV footage was securely deleted.

8.2.2. CCTV footage will be retained for as long as required where it serves as evidence of matters such as those set out in Section 5.1 above, as identified by the Authorised Person or his / her nominee(s).

8.2.3 In the event that CCTV footage is to be retained the following procedure will apply:

- the relevant footage will be downloaded onto an appropriate storage device by the Authorised Person or his / her nominee(s) and retained in a secure location;
- the copy will be securely retained until written confirmation from the relevant Director of Service / Head of Function is received to confirm that the matter is concluded. Upon receipt of such confirmation, the footage will be securely deleted by the Authorised person or his / her nominee(s).

8.2.4. Hard copy print outs of CCTV footage are subject to the same controls as those set out above.

9. Request for Access to CCTV Footage

9.1 Access to recorded footage is restricted and carefully controlled to make sure that the rights of individuals are preserved and that the chain of evidence remains intact should the footage be required for such purposes.

9.2 A log of access to tapes / images will be maintained by the Traffic Management Centre or by the relevant department for CCTV systems which are not monitored by the Traffic Management Centre.

9.3 Any person whose image has been recorded has a right to request a copy of the information recorded on request, provided such an image / recording exists and has not been deleted.

9.4 Requests by data subjects for access to their personal data captured in CCTV images must be made in writing to the Data Protection Officer, Corporate Performance and Change Management, South Dublin County Council, County Hall, Town Centre, Tallaght, Dublin 24 within the retention period specified in 8.1.1. above. Recorded footage will only be disclosed in consultation with the Traffic Management Centre Controller and/or the Authorised Person of the relevant CCTV System. Such disclosure will be in compliance with the Data Protection Acts 1988 to 2018 and with the Council's Data Protection Policy and Staff Guidelines.

9.5 South Dublin County Council must respond to such requests within one month of receipt of the request.

9.6 A person should provide all the necessary information to assist the Council in locating the CCTV recorded data, including the date, time and location of the recording. If the image is of such poor quality as to not clearly identify an individual, that image may not be considered to be personal data and may not be provided by the Council to the requesting party.

9.7 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. Any images of other individuals must be obscured before the data is released. The data subject must be provided with details of the purpose of the CCTV system, other organisations with which the images may be shared, contact details of the Council's Data Protection Officer and be advised of his/her data subject rights as detailed in the Council's Data Protection Guidelines and right to make a complaint to the Data Protection Commission in relation to the processing of his/her personal data.

9.8 If An Garda Síochána requests CCTV images for a specific investigation, the Data Protection Officer / Authorised Person must satisfy himself / herself that there is a criminal investigation underway or that the images are required for specified crime prevention purposes. A request from An Garda Síochána should be in writing on Garda headed notepaper, signed by a Garda not below the rank of Inspector, should clearly identify the legal basis under which access is requested and confirm that the requested CCTV images are required for the purposes of a criminal investigation or for specified crime prevention purposes . All requests made by An Garda Síochána will be recorded in the Access log and copies of the formal request should immediately be sent to the Council's Data Protection Officer in all cases followed by confirmation of the date of release of CCTV images. The CCTV images released must be in secure encrypted format.

9.9 Requests from other law enforcement authorities such as the Competition and Consumer Protection Commission should be handled in a similar manner to requests from An Garda Siochana and subject to similar controls and the requirement to identify a clear legal basis for seeking access to CCTV images. The CCTV images released must be in secure encrypted format.

9.10 Requests made by departments within the Council for access to CCTV

images held by another department must be in writing, signed by a person not below the level of Senior Executive Officer or analogous grade, clearly identify the legal basis under which the request is being made and outline the purpose for which the CCTV images are required which must satisfy the requirements of the Data Protection Act 2018.

Copies of all such requests should immediately be forwarded to the Council's Data Protection Officer and confirmation subsequently provided of the decision made on the request and date of release of CCTV images where applicable.

9.11 Copies of CCTV images provided in response to requests should be provided in an encrypted format in order to minimise the risk of data breaches.

10. Security Companies

10.1. Where a Council owned premises CCTV system involves data processing by a Security Company contracted by the Council, the following applies:

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

10.1.2. Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors". As data processors, they operate under the instruction of data controllers (their clients). South Dublin County Council is the data controller for the CCTV systems covered by this Code Of Practice. The Data Protection Acts 1988-2018 and the General Data Protection Regulation 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;

10.1.3.Staff of the security company must be made aware of their obligations relating to the security of data and a data processing agreement must be in place between the Council and the relevant company. No sub-contracting of data processing responsibilities by security companies in their role as data processors on behalf of the Council can take place without the express prior written agreement of the Council. In the event of such sub-contracting being authorised by the Council a separate data processing agreement must be entered into between the data processor engaged by the Council and the sub-processor before any data processing by the sub-processor occurs.

11. Data Protection Impact Assessments

The Data Protection Commission has provided guidance to the effect that all CCTV involving ongoing and widescale monitoring of data subjects is considered high risk and it is a requirement therefore that a Data Protection Impact Assessment be done before any new CCTV systems are commissioned. Full consideration must be given to the use of alternative methods of achieving the desired outcome before a decision is made to commission a new CCTV system.

12. Review of existing CCTV systems

Existing CCTV systems should be regularly reviewed by reference to the purposes for which they were originally commissioned and evaluated in the context of whether the intended outcomes have been achieved and whether the outcome could be achieved by an alternative method. Changes to existing CCTV systems involving the use of new technology will require the preparation of a Data Protection Impact Assessment.

13. Implementation and Review

This Code of Practice will be reviewed on foot of changing legislation or guidelines (for example, from the Data Protection Commission, An Garda Síochána, internal or external audit recommendations).

An evaluation of its implementation will be carried out every three years lead by the Director of Corporate Performance and Change Management or his / her nominee and will include consultation with each relevant department and all named Authorised persons.

14. Personal data breaches

All personal data breaches arising from the processing of data through the use of CCTV must be brought to the attention of the Council's Data Protection Officer immediately along with a detailed report in relation to the breach.

15. Non-Compliance with this Code of Practice

Non-compliance with the procedures contained in this Code of Practice may result in initiation of the Council's Grievance and Disciplinary Procedure.