Comhairle Contae
Átha Cliath Theas
South Dublin County Council

South Dublin County Council CCTV and other Surveillance Technology Policy

("CCTV POLICY")

Version	Author	Date	Changes	Reviewed by	Approved by	Applicable from
1.0	Sarah Hartnett, DPO	10.11.23	Initial draft	Michael Murtagh SEO	Senior Management Team	25.03.2024

Table of Contents

1. Introduction

This document sets out the South Dublin County Council Policy (hereinafter "Policy") in relation to the use of Closed-Circuit Television (CCTV) and other Surveillance Technology Systems (hereinafter collectively referred to as "**CCTV Systems**" and further defined in Section 5," Definitions" below).

As the local government authority for South Dublin, South Dublin County Council (hereinafter "SDCC" or the "Council") processes personal data captured by CCTV Systems, strictly in accordance with the General Data Protection Regulation (GDPR), the Data Protection Acts 1988- 2018 and the guidance provided by the Data Protection Commissioner (See Appendix I).

The CCTV Systems operated by SDCC generally serve four main purposes: Community CCTV System Schemes in public areas, Traffic Management CCTV Systems, Waste Enforcement CCTV Systems and Property CCTV Systems for Council-owned premises and assets.

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

Community CCTV Systems operate in public places such as greenways, walkways, on streets, on roadways, bridges, in some estates and/or parks, at town centres and other public places where the public has either an implied or express, right of access. A proportion of our Community CCTV Systems are real-time monitored by a third-party services provider at a dedicated monitoring centre. Retrospective monitoring is carried out upon request from An Garda Síochána or in receipt of a valid data access request.

Road Traffic CCTV Systems may operate at major road junctions and/or for the purpose of safe and efficient management, operation and use of public roads, including traffic management and providing information to the public Road Traffic CCTV Systems may also operate at other locations for set periods of time at certain accident blackspots or high-risk areas in order to determine the appropriate traffic management measures required.

Waste Management CCTV Systems may operate in the functional areas of SDCC for the purpose of deterring environmental pollution, and/or facilitating the deterrence, prevention, detection, and prosecution of offences under this Act.

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.

2. Purpose of this Policy

2.1. The purpose of the SDCC CCTV Systems Policy is to establish clear provisions that enable SDCC to fulfil its data protection obligations concerning the operation of CCTV Systems. This Policy encompasses various aspects including, but not limited to, the application and approval process for CCTV Systems, rules relating to the location, monitoring, control and security of CCTV systems, recording by CCTV systems and access to such recordings.

2.2. Specifically, this Policy serves the following key purposes:

- **Clarity of Purpose:** To specify the reasons and methods through which SDCC employs CCTV Systems and how data processed by these CCTV Systems is processed.
- **Data Protection:** To ensure that the rights of individuals whose personal data is captured by SDCC's CCTV Systems are recognized and safeguarded in accordance with the

applicable Data Protection Legislation.

- **Legal Compliance:** To assist SDCC Employees in adhering to their legal obligations when engaging CCTV Systems, including adhering to all applicable Codes of Practice, as well as when handling personal data obtained through SDCC CCTV Systems.
- **Respecting Rights:** To specify the procedures by which individuals can exercise their rights concerning personal data generated by SDCC's CCTV Systems, promoting transparency and accountability.
- **Ensuring legitimate Access:** Setting out the requirements for requests from members of An Garda Síochána, Council staff and Members of the public who seek to access CCTV recordings and associated data processed via SDCC CCTV Systems.

Through this Policy, SDCC aims to strike a balance between enhancing security and respecting individual privacy rights while fostering a culture of responsible data management and compliance with the applicable laws and regulations.

3. CCTV Video Monitoring and Recording Purposes

3.1. CCTV Systems in this Policy refers to video and similar surveillance technology recording systems that may be used by SDCC for the following purposes:

- To protect and safeguard the health and safety of Council staff, elected members, customers, visitors and contractors.
- To safeguard and protect the security of premises both internally and externally and the plant, equipment and property, parks, pavilions and cemeteries and all other assets under the ownership and remit of the Council.
- To assist in the maintenance of public order and safety in public places.
- To improve public and community safety and perception of safety by the local communities by assisting in the prevention, detection and investigation of offences, in turn assisting in the prosecution of offenders.
- To prevent, detect and investigate crime and illegal activities and in order to assist in the prosecution of offences Criminal Investigations by An Garda Síochána (AGS).
- Investigation by Council management of reported incidents/accidents and of suspected, or allegations of fraudulent behaviour or other activities consistent with this Policy.
- Investigations carried out by other agencies in relation to incidents, i.e. Health and Safety Authority, the Council's Insurers and or legal advisors.
- Raising awareness for members of the public interacting with staff on Council premises that their actions are being recorded in order to deter offences, e.g. assault and bodily harm.
- To help create a cleaner environment and public spaces by identifying and combating illegal dumping.
- To help with better traffic management and control, traffic counting and categorisation, traffic flow.
- Other purposes as may arise from time to time and as will be assessed on a case-by-case basis.

CCTV Systems will only be considered by SDCC where their use is necessary and proportionate, and data obtained using CCTV systems shall be limited and proportionate to the purposes for which it was obtained. The specific purpose for which CCTV Systems are actually operated by the Council shall be included in the relevant privacy policy.

3.2. CCTV Systems will not be used by the Council to monitor employee performance. It may however, on specific occasions while adhering to the applicable internal processes, protocols and codes of practice, be used in the investigation of complaints and disciplinary matters. For the avoidance of doubt, CCTV monitoring/profiling of an individual based on any of the following characteristics is prohibited by this Policy; Age, Civil status, Disability, Family status, Gender, Race, Religion, Sexual orientation, Membership

of the Travelling Community.

4. Scope

4.1. This Policy applies to:

- SDCC Employees but especially Data Users (as defined in Section 5, **Definitions**, below)
- SDCC uses of CCTV Systems
- CCTV Systems service providers (Data Processors) contracted by SDCC
- Joint Data Controllers alongside SDCC
- All individuals/organisations acting on behalf of SDCC as regards CCTV Systems

5. Definitions

5.1. Any Terms used or referred to in this Policy, which are not defined below, shall have the meaning attributed to them by the EU General Data Protection Regulation (GDPR).

5.2. For the purposes of this Policy, the following terms have the following meanings:

- CCTV refers to Closed Circuit Television Systems, which are fixed, and Pan-Tilt-Zoom (PTZ) cameras designed to capture and record images of individuals and property.
- CCTV Systems refers to 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 similar systems that capture information of identifiable individuals or information relating to identifiable individuals.
- CCTV Authorised Persons refers to Employees of the who are authorised to access CCTV footage for specific purposes and who have undergone specific CCTV Data Protection Training. The list of current Authorised persons is maintained by the Directorate CCTV Coordinator.
- The "Council" or "SDCC" refers to South Dublin County Council.
- CCTV Authorised Persons: refers to those members of staff that have been tasked with completing a CCTV related task by their relevant SEO and / Or Director of Services. They are usually the CCTV Directorate Coordinator or their support staff.
- CCTV System Monitoring Centre refers to the monitoring centre or control room established to receive and maintain the CCTV footage. For the operation of the Monitoring Centre an SDCC operation manual applies and must be adhered to at all times.
- Data refers to information which is stored electronically, or in certain paper-based filing systems.
- Data controller(s) as defined by the GDPR, are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law.
- Data processors: means any person or organisation that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).
- Data subjects: means all living individuals about whom we hold personal information as a result of the operation of our CCTV Systems.
- Data Users: are those employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve, transfer, and delete images. Data users must protect the data they handle in accordance with this Policy and the SDCC 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, viewing, collecting, storing 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, including tools or contractors.

6. Roles and Responsibilities

The responsibility for CCTV within the Council is delegated as follows:

Senior Management Team	Receives regular reports from the CCTV Oversight Board, determines the CCTV strategy of the Council.
CCTV Oversight Board Sponsors	Members of the Senior Management Team with CCTV System operations owned / managed by their directorate. They Sponsor and nominate the members of the CCTV Oversight Board.
CCTV Oversight Board	The CCTV Oversight Board is a cross-departmental working group established by the Council's Senior Management Team to support the implementation of the CCTV Policy. The CCTV Oversight Board reports to the Senior Management Team. The DPO is consulted as a member of the Oversight Board. The Board reviews all CCTV Systems, cameras and their functionality at least on an annual basis. The CCTV Oversight Board will meet quarterly to review the live monitoring status of cameras. The general role of the CCTV Oversight Board Members requires them to have full knowledge, understanding and oversight of CCTV operations within their sections and within their directorate. They must have the clear authority to direct the implementation of compliance with all Data Protection Legislation and resulting CCTV System requirements in their directorate as regards CCTV and similar surveillance technology systems.
Directorate CCTV Coordinator	The Directorate CCTV Coordinators report to the CCTV Oversight Board and are responsible for the daily operations of the CCTV Systems within their Directorate in line with this Policy and as directed by the Member of the CCTV Oversight Board that they report to.
CCTV Authorised Persons	Members of staff that have been tasked with completing a CCTV related task by their relevant SEO and / or Director of Services and / or the Directorate CCTV Coordinator. They are usually the Support Staff of the Directorate CCTV Coordinator.
Nominees	Nominee(s) are authorised by the Director of Services to operate and monitor a particular CCTV System (e.g., a contractor). All Nominees that operate and/or monitor community CCTV Systems must be non-Act Garda vetted.
Data Protection Officer	Appointed by the Council, who will monitor compliance with the Council's data protection obligations concerning the operation of its CCTV Systems and advise the Council on the operation of such from a data protection perspective.

CCTV Oversight Board

The broad remit of the CCTV Oversight Board is to support the Chair of the Oversight Board in providing overall direction and management for CCTV projects according to the overall CCTV Strategy provided by the Senior Management Team and the Data Protection Requirements, as advised by the Data Protection Officer. Any proposed changes as deemed necessary by AGS or the Council in relation to CCTV Systems must be considered by the CCTV Oversight Board.

CCTV Board Structure
The CCTV Oversight Board is structured as follows:

CCTV Oversight Board Sponsors:

- Director of Economic, Enterprise and Tourism Development
- Director of Housing, Social and Community Development
- Director of Environment, Water and Climate Change
- Director of Land Use, Planning and Transportation
- Director of Corporate Performance and Change Management
- And/or other Directors /Heads of as determined by the Chief Executive

CCTV Oversight Board Members:

- Head of ICT* (Independent Digital Oversight)
- Senior Architect* (Independent Oversight)
- Senior Executive Officer* Housing
- Senior Executive Officer* Social, Community, development
- Senior Executive Officer* LUPT
- Senior Executive Officer* EETD
- Senior Executive Officer* EWCC
- Senior Executive Officer* CPCM
- County Librarian*
- Data Protection Officer (Independent Data Protection advisor)

** and /or analogous and / or Senior Engineer (SE) and / or those acting in that position, and /or those deemed to be sufficiently senior managers in charge of Business Units by the relevant CCTV Oversight Board Sponsor(s).*

CCTV Oversight Board Duties and Responsibilities
The CCTV Oversight Board is responsible for the following:

- Act in accordance with the CCTV Oversight Board Terms of Reference.
- Review CCTV related Policies and standards.
- Authorise and prioritise SDCC CCTV projects. "Authorise" in this sense refers to assessing of the necessity and proportionality (See Appendix V below) for a CCTV Proposal submitted to it by Business Units or by Authorised Persons, prior to the Oversight Board recommending the CCTV Proposal to the Chief Executive of the Local Authority for full and final approval. All CCTV System applications, changes and decommissioning must be accompanied by an up-to-date Data Protection Impact Assessment which has been approved by the DPO and the Director of Services. The relevant Directorate CCTV Coordinator will be tasked by the applicable CCTV Oversight Board Member with coordinating the completion a DPIA and submitting it to the Board for review.
- Review all current SDCC CCTV Systems, ensure compliance with Data Protection Legislation and issue recommendations in that respect.
- Conduct an annual audit of all CCTV locations, processes and procedures.
- Meet bi-annually to review the live monitoring status of cameras. The CCTV Oversight Board will review the live monitoring status of cameras. A determination will be made as to which cameras should continue to be live monitored and which cameras should no longer be monitored. On occasions when not being actively monitored by an operator, all operating cameras should be placed in the most advantageous position to record any incidents occurring in a public area within its field of vision.
- Report regularly to the Senior Management Team via the Chair of the CCTV Oversight Board, at the very least after every sitting of the CCTV Oversight Board and as directed by the Senior Management Team.
- Where their Directorate commissions and/or operates CCTV Systems, the relevant CCTV Oversight Board Member must nominate a CCTV Directorate Coordinator for their Directorate who will regularly report to them on the daily operation of the CCTV Systems within their Directorate.

- Where the Oversight Board has endorsed a CCTV Proposal, it shall then be submitted to the Chief Executive for consideration, and final decision by means of formal written approval.

CCTV Directorate Coordinators

- The CCTV Directorate Coordinators are nominated by the relevant CCTV Oversight Board member within the Directorate, and report to the CCTV Oversight Board via said member. They are responsible for the daily operations of the CCTV systems within their Directorate in line with this Policy and as directed by the CCTV Oversight Board Member.
- The CCTV Directorate Coordinators monitor the operation of the CCTV system and cameras on an ongoing basis and call upon the contractors/ Data Processors and CCTV Authorised Persons as required.

CCTV Directorate Coordinators Duties and Responsibilities

The main duties and responsibilities of the CCTV Directorate Coordinators are as follows:

- Ensure that the use of CCTV is implemented in accordance with this Policy.
- Ensure the completion of Data Protection Impact Assessments for all CCTV Systems within their remit.
- Oversee and co-ordinate the use of CCTV for safety and security purposes within the Council as directed by the CCTV Oversight Board, their SEO and/or Senior Management and provide regular reports to the CCTV Oversight Board as directed by their SEO.
- Maintain the list of CCTV installation requests, internal and external, and make recommendations for new camera/CCTV System installations in line with the CCTV Policy.
- Liaise with the DPO regarding the CCTV Authorised Persons List and maintain the Directorate CTV Authorised Persons List. This list is to be included in the Directorate's Surveillance Device Inventory Table.
- Maintain the CCTV Access Procedure as described in this Policy and in Annex IV to this Policy.
- Maintain the record of CCTV download requests (*see Appendix III for CCTV Download Request form template*) for their Directorate and provide statistics on such to the DPO for quarterly reports to the CCTV Oversight Board.
- Ensure that the CCTV installations are compliant with this CCTV Policy and answer any further questions in that respect as posed by the CCTV Oversight Board and/or the DPO.
- Ensure that all existing CCTV are evaluated for compliance with this Policy.
- Maintain the CCTV asset register for their Directorate (Directorate's Surveillance Device Inventory Table).
- Ensure that the CCTV monitoring by the Council is consistent with the highest standards and protections.
- Co-ordinate and support the release of recorded CCTV data in compliance with this Policy and data protection legislation.
- Maintain a record of access (i.e., an access log, See Appendix IV Access Log for requirements) to, or the release of footage or any material recorded or stored in the system(s).
- Ensure that no copies of recordings are made without authorisation.
- Ensure that the perimeter of view from fixed location cameras conforms to this Policy both internally and externally.
- Ensure that all areas being monitored are not in breach of an expectation of the privacy of individuals and be mindful that no such infringement is likely to take place. Where a risk is identified the DPO is to be consulted and the risk is to be brought to the relevant SEO's attention immediately.
- Advise, in conjunction with the DPO, on the Council's cameras (excluding Community CCTV Scheme cameras) to ensure they are non- intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "reasonable expectation of privacy".
- Ensure CCTV footage is stored in a secure place with access by authorised personnel only.
- Ensure that images recorded are stored for a period of no longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the CCTV Oversight Board.
- Ensure that all financial obligations for operations and maintenance are traceable and auditable.

- Regularly consult with the DPO when and where appropriate.
- Conduct regular audits of CCTV Access Logs (see Appendix IV Access Log for exact requirements of an Access Log), CCTV Contractors etc. with and as advised by the DPO.
- Regularly report to their Directorate CCTV Oversight Board Member as to the status and operation of CCTV Systems within the Directorate.
- To delegate and assign CCTV System related tasks as appropriate to CCTV Authorised Persons.

CCTV Authorised Persons Duties and Responsibilities

- For each CCTV System, the CCTV Oversight Board Member and their appointed Directorate CCTV Coordinator may identify the CCTV Authorised Persons within the Directorate 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 Directorate's Surveillance Device Inventory Table and forwarded to the CCTV System Monitoring Centre.
- All CCTV Authorised Persons and nominees will be appointed by Chief Executive Order.
- CCTV Authorised Persons are responsible for making sure that the system is only used in an appropriate manner in conformance with legislative requirements and this Policy and as directed by the CCTV Oversight Board.
- CCTV Authorised Persons 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. Data Protection Impact Assessments

7.1.It is compulsory to undertake a Data Protection Impact Assessment (DPIA) in advance of installing or making adaptations to any (or part of) Council CCTV Systems, even if the change simply involves the addition of a camera, changes to the positioning of the camera and subsequent view and/or disabling of cameras.

7.2.Should a Section/Directorate discover that a DPIA does not exist for a specific camera, drone or other CCTV Systems, they will immediately inform the relevant SEO, the DPO and immediately halt such processing until such time as the DPIA has been completed and the CCTV System has been authorised by the CCTV Oversight Board.

7.3. The SEO of the Section or Directorate proposing the CCTV System or changes thereto, will nominate a responsible person to conduct the DPIA and to report on its status to the Directorate CCTV Coordinator. The nominated person will inform the Directorate CCTV Coordinator and the DPO that a DPIA has commenced. The most UpToDate DPIA template is to be used and can be obtained from the DPO.

7.4.The purpose of a DPIA is to facilitate the identification and implementation of appropriate measures to eliminate or minimise any risks arising out of the processing of personal data by a CCTV System.

7.5. A draft DPIA must be submitted to the Data Protection Officer for review and the final CCTV System request including the completed DPIA (as authorised by the appropriate Director of Services) must be submitted to the CCTV oversight Board for authorisation. DPIA's must be reviewed annually or more often if changes to the processing are introduced.

8. Business Case Rationale

8.1. Requests for CCTV Installations submitted to the CCTV Oversight Board must include a business case rationale, which has been approved by the appropriate Director of Services requesting the installation as project sponsor. The business case rationale will indicate that allocation of funding for installation and annual funding for maintenance, communications, and monitoring costs has been provided for. As such,

the business case rationale must also be approved by the Head of Finance or a nominated officer.

9. Community Based CCTV

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

9.2. The following conditions must be fulfilled in order to obtain authorisation from the Garda Commissioner:

- The CCTV scheme must be approved by the local authority after consultation with the Joint Policing Committee for its administrative area.
- The CCTV scheme must comply with technical specifications issued by the Garda Commissioner and be operated in accordance with the Code of Practice.
- A submission and presentation must be made to AGS CCTV Advisory Committee that consists of three Chief Superintendents working in specialised areas and the DPO of AGS. At this meeting, AGS will either approve or decline the application, or make a request for updates or additional information, pending approval.
- Members of An Garda Síochána will be given access at all times to the CCTV system upon written request in accordance with the agreed procedures.
- The local authority gives an undertaking that it will act as a joint controller in respect of the Garda authorised and approved Community Based CCTV Schemes.

10. CCTV Locations

10.1. The location of cameras and other Surveillance Technology is a key consideration which must be documented in the DPIA, with particular reference to:

- the number of cameras/surveillance devices selected,
- how that specific number fulfils the purpose and is balanced against the privacy rights of the public/any potential data subject,
- the type of camera/technology selected,
- how it fulfils the principles of Data Protection, as well as the
- specific location of each camera or surveillance device and the factors that have determined the suitability of that location. The Council will document in the DPIA its considerations in selecting locations for the installation of CCTV Systems which are least intrusive to protect the privacy of individuals. Cameras are positioned in such a way as to prevent or minimise the recording of such places to the greatest extent possible.

10.2. Use of CCTV Systems to monitor areas where individuals have a reasonable expectation of privacy is prohibited. As a rule, cameras / surveillance devices that record external/public areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

10.3. At all times, CCTV Systems are to be utilised in a fair and ethical manner.

10.4. Wherever possible, privacy masking is applied on CCTV cameras, in order to block-out areas where individuals have a reasonable expectation of privacy.

10.5. Video monitoring of public areas and within the Council's public offices & premises for security and

health and safety purposes, is restricted to uses that do not violate the individual's reasonable expectation of privacy. CCTV will not be located in areas where staff and the public would expect privacy such as break rooms, changing rooms, showers and toilets.

11. CCTV System Signage

11.1. In accordance with Article 12 and 13 of the General Data Protection Regulation (GDPR) as transposed into the Data Protection Legislation, the Council as a Data Controller shall take appropriate measures to provide any information relating to processing (in advance of processing) to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. As concerns CCTV Systems, the Council fulfils the requirements of the applicable Data Protection Legislation via installing appropriate signage and keeping the relevant privacy statements available and up to date.

11.2. The placement and amount of CCTV System Signage, as well as the suitability of such to fulfil the legal requirements as detailed in 11.1 is analysed in advance of processing and installation, and the analysis and conclusions thereon are detailed in the relevant DPIA, in advance of implementing CCTV Systems.

11.3. CCTV System signage is to be recorded in a CCTV System Signage Register which is maintained by the Directorate CCTV Coordinator and which details: the date signage was erected, text included on the signage, geographical location of the signage, date upon which the signage was last inspected, notes from the inspection, follow up actions and completion dates. Inspections must occur at least once quarterly, and any discrepancies are to be addressed by the Directorate concerned and logged in the CCTV System Signage Register. A copy of the register is to be provided to the DPO once a year for review and/or upon request and it is available for inspection at any time by the DPO and the CCTV Oversight Board.

11.4. CCTV System signage is to be placed at locations where CCTV camera(s) are located, as well as on the roads and walkways/greenways/ entrances and/or hallways leading to that area. Signage must be clearly visible and legible to members of the public and includes the name and contact details of the Data Controllers, link to the relevant privacy Policy, as well as the specific purpose(s) for which the CCTV camera is in place in each location. CCTV which is also monitored by An Garda Síochána must clearly indicate that such monitoring takes place on the signage provided.

11.5. Appropriate locations for signage include:

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

12. Covert Surveillance

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

12.2. The decision to utilise covert surveillance must be carried out in accordance with this Policy. The Data Protection Officer must be consulted in advance of any planned covert surveillance and the operation of any such covert surveillance will be subject to a Data Protection Impact Assessment prior to

commencement of processing. The Business Case and DPIA for the intended covert surveillance must be approved in advance of utilization of covert surveillance by the relevant Director of Service. Permission of the Chief Executive (CE) in text form must be obtained before considering covert surveillance.

12.3. The use of covert CCTV may result in the initiation of legal proceedings. The recommendation to proceed with covert CCTV for this purpose must be supported by documentary evidence of the incidents which have led to the decision to proceed with same.

12.4. Covert surveillance is to be focussed, and of the minimum duration possible, as analysed in the Data Protection Impact Assessment. Only specific and relevant locations/individuals will be recorded. Limited numbers of people will be involved in any covert surveillance.

13. Record Retention

13.1. 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". For all SDCC CCTV Systems a maximum retention period of 28 days applies, unless there are specific, legitimate and reasonable grounds for the retention of images beyond that period, which are documented and the documentation is submitted to the DPO and the CCTV Oversight Board for prior approval. The envisioned retention period will be analysed and that analysis included in the relevant Data Protection Impact Assessment.

13.2. At the end of their retention period, recordings and images will be erased permanently and securely. Any physical matter will be disposed of as confidential waste. A Deletion log is retained, detailing the general data that has been deleted, the dates it concerned, the cameras concerned, the person completing the deletion and any relevant notes etc. Data Processors must provide a deletion log to the Council for every deletion routine that they carry out on behalf of the Council.

14. Technical and Organisational Measures

14.1. General Access: CCTV footage must be stored in secure environments and access will be restricted to authorised personnel only. An access log (see Appendix IV) must be maintained and made available for inspection on request from the Data Protection Officer. An audit report of the access logs is provided to the DPO on a quarterly basis.

14.2. Supervising the access and maintenance of the CCTV System is the responsibility of the CCTV Coordinator and the Directorate CCTV Officers.

14.3. Integrity and Security: In order to ensure that the rights of individuals recorded by the CCTV system are protected, the Council ensures that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This includes encrypting the data where it is possible to do so. The Council shall ensure that appropriate access controls are put in place in respect of CCTV System footage / image storage including robust encryption where remote access to live recording is permitted.

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

14.5. All recorded CCTV footage must be adequately secured and access to playback of recorded footage must be password controlled. Sharing of passwords is not permitted and each CCTV Authorised Person authorised to access footage has their own unique credentials, including a username and password. Such credentials conform to the SDCC requirements for passwords.

14.6. Each Directorate is individually responsible for the procurement, technical operation and maintenance

of CCTV Systems under their remit.

14.7. Recording by staff or appointed Data Processors of any CCTV System footage / images on mobile phones or other video recording devices is strictly prohibited.

15. Footage from CCTV Systems retained as Evidence

15.1. The following log of retained recorded CCTV System footage will be maintained by the named CCTV Authorised Persons or his / her nominee(s), as set out in Section 6 of this Policy:

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

15.2. In all cases, CCTV System footage will only be retained for as long as required where it serves as evidence, as identified and documented by the CCTV Authorised Person and or his / her nominee(s).

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

- An appropriate access request will be submitted to the DPO, as outlined in Section 16 below.
- The relevant footage will be downloaded onto an appropriate, encrypted 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 / SEO is received to confirm that the matter is concluded. Upon receipt of such confirmation, the footage will be securely deleted by the CCTV Authorised Persons or his / her nominee(s) and a deletion log is retained by the CCTV Authorised Person and provided to the Directorate CCTV Coordinator.

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

16. Accessing and Downloading CCTV Footage

16.1. Data will only be shared with third parties where the Council has a lawful basis to do so and only in accordance with this Policy.

16.2. All access requests must be submitted to the DPO alongside the Directorate/section analysis as to the legitimacy of the request, the legal basis for the request, the proportionality and necessity of sharing the CCTV footage and any other legal requirements that may apply.

16.3. A centralized record of all disclosures of CCTV footage is held by the Directorate CCTV Coordinators, which includes all requests received by that Directorate, whether it was accepted / denied / rejected, the necessity and proportionality test conducted (See Appendix V below), the legal basis for the release, record of DPO approval of the request.

16.4. Access may be provided to the following subject to the terms of this Policy:

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

for Access to CCTV Footage

16.5. 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.

16.6. Access by Data Subjects

- **(i)** Data protection legislation provides data subjects with a right to access their personal data *(See Appendix II Data Subject Access Request Form*). This includes their recognisable images and other personal data captured by CCTV system recordings. Access requests are encouraged to be made electronically (via email) however all requests made in writing/by email/verbally to the Data Protection Office will also be accepted provided all necessary information is supplied. However, where an access request is made verbally, the Council's Data Protection Officer would encourage individuals to submit email/ written access requests where practical, to avoid disputes over the details, extent, or timing of an access request. All data subject access requests must be submitted to the Data Protection Office (dataprotection@sdublincoco.ie).
- **(ii)** In seeking access to their Personal Data, it will be necessary for the Data Subject / requester to submit their own photographic ID in order to ensure that it matches with that on the CCTV recordings. Verification will be conducted by the SDCC Data Protection Office. An access request is deemed to be verified where the requester has verified their identity to the Council's Data Protection Office via providing a form of photo identification (e.g., Passport, driver's licence, Public Services Card).
- **(iii)** In giving a person a copy of their data, the Council may provide a copy of the footage in video format or where it is not technically possible to do so, provide a still or series of still pictures or a disk with relevant images. If the image is of such poor quality so as not to clearly identify an individual, that image may not be considered to be personal data and may not be released by the Council. If there are images and/or other personal data of other individuals (not the data subject) on the recording these must be obscured/pixellated before the data is released unless consent has been obtained from those other parties to their release. If the CCTV recording no longer exists on the date that the Council receives a verified access request, it will not be possible to provide access to a data subject.

16.7. Access Requests from an Garda Síochána to Council CCTV System Footage

- **(i)** Request for copy of recording/download or viewing: The viewing/handing over/downloading of CCTV System footage to An Garda Síochána requires a formal written communication (CCTV Access Request Form) confirming that the material is sought for the prevention, investigation or detection of a crime, alongside the legislation under which the offence is being investigated). A log of all An Garda Síochána requests is maintained by the DPO and all such requests must be submitted to the DPO alongside the necessity and proportionality test (See Appendix V below) conducted by the recipient of such a request in the council. All such requests are to be submitted to the relevant Senior Executive Officer for approval/denial, subsequent to review by the DPO.
- **(ii)** All requests made by An Garda Síochána must be on An Garda Síochána headed paper, quote the PULSE unique number, include the details of the CCTV footage required, cite the legal basis for the request, as well as the legislation under which the offence is being investigated. The access request form submitted by An Garda Síochána must be signed by a member of Superintendent or Inspector rank to authorise the request.
- **(iii)** The Council CCTV Authorized Person that processes the request and submits it to the DPO and subsequently their SEO for approval, will conduct and document a proportionality and necessity test in accordance with the requirements of Section 41(b) of the Data Protection Act 2018 and submit such to the DPO. Guidance is available from the DPO on such tests (See Appendix V below). The SDCC internal CCTV Access Request Form can be found in Appendix III below.

- **(iv)** Where any such requests are made directly to the Data Processor instead of the Council, the Data Processor must direct An Garda Síochána to contact the Council as Data Controller and the Data Processor maintains a log and provides a copy to the Council. This log is available for inspection by the Council at all times.
- **(v)** Emergency requests: In order to expedite a request in urgent situations, a verbal request from An Garda Síochána to access CCTV recordings will suffice. This should only happen in exceptional circumstances and does not negate the necessity to submit the request to the DPO for approval from a data protection perspective and to conduct a necessity and proportionality test (See Appendix V below), and to submit to the relevant Senior Executive Officer for final approval. Such a verbal request must be followed up with a formal written request from An Garda Síochána within 24 hours. The request form must include the details outlined in section (ii) above.

16.8. **Access by CCTV Authorised Persons:**

- (i) CCTV footage can only be accessed by designated Council staff members who are known as CCTV Authorised Persons. In order to access Community CCTV Schemes, designated staff members and/or contractors must be non-Act Garda vetted. Non-Act vetting is Garda Vetting conducted on behalf of organisations registered with this unit, outside of the framework set down in the National Vetting Bureau (Children and Vulnerable Persons) Acts 2012 to 2016. Please contact the DPO to commence this process. CCTV Authorised Persons are authorised to view CCTV footage.
- (ii) Downloading of footage requires an access form (Appendix III) to be completed and the access must be approved and logged with the Data Protection Officer, and subsequently approved by the relevant SEO.
- (iii) Download requests must be on Council headed paper, detail the CCTV footage required and must also cite the legal basis for the request, i.e. the Act, Section, etc. under which the request is made, as well as the proportionality and necessity (See Appendix V below) for the request. The requester must ensure that the request complies with: Data Protection Legislation, the underlying legislation under which the request is made and this CCTV Policy. The DPO will approve the CCTV Download Request (See Appendix III) and return the signed CCTV Download Request to the CCTV Authorised Persons only when satisfied that all the conditions have been met. The CCTV Authorised Person will then submit the request to their SEO for final approval. The CCTV Authorised Persons must keep a copy of the approved CCTV download request (Appendix III)in the Directorate inspection record retained by the Directorate CCTV Coordinator and present the original approved CCTV request to the CCTV System Monitoring Centre in order to obtain the footage.
- (iv) The CCTV System Monitoring Centre must retain the original signed CCTV download request (Appendix III) for a period of no less than 5 years. For audit and verification purposes a record must be maintained by the Council on all CCTV download requests regardless of whether they are approved or not.
- (v)The DPO will report to the CCTV Oversight Board on an annual basis as regards: Total Number of CCTV download requests, number of CCTV download requests approved, number of CCTV download requests rejected.

16.9. Third Parties: From time to time the Council may share CCTV System recordings with its advisors, for example, its insurers and its legal advisors for the purposes of obtaining legal advice, resolving disputes and defending, compromising or otherwise settling litigation. The provision of access to such third parties is also included in the access request log maintained by the DPO and all requests must be submitted to and approved by the DPO.

16.10. Monitoring Services, Security and IT Support, CCTV System Administration and Maintenance Providers: Third party services providers, so-called “data processors” are contracted to process Personal Data including CCTV System footage on behalf of the Council. These Data Processors receive access to CCTV

System footage in order to provide the contracted services to the Council. The access is strictly limited to what is necessary in order for the Data Processor to fulfil their contract with the Council. The Council always enters into an appropriate Data Processing Agreement with the Data Processor, prior to processing and regular auditing of such Data Processors is conducted by the Council.

16.11. Other Parties: The Council may also provide access in circumstances where a data subject gives consent or instructs the Council to do so (e.g. to a solicitor or union representative etc.), or where we are otherwise legally required to do so (e.g. on foot of a Court Order).

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

17. Directorate Surveillance Device Inventory Log

17.1. A CCTV System Register known as the Directorate Surveillance Device Inventory Log is maintained by the Directorate CCTV Coordinator. The system used to maintain the Council's CCTV System register is controlled by Corporate Service.

17.2. This register contains at least the following information:

- Location and GPS coordinates of each CCTV system
- Live Recording/Monitoring status
- Masking Status
- Make and model of each CCTV System
- Legal Basis for each CCTV System
- CCTV System service provider details
- Data sharing / Joint Controllership status
- Retention period for CCTV recordings
- Signage register details
- Details of Authorised CCTV Persons having responsibility for and/or access to each CCTV system
- DPIA status
- RoPA status
- Access Log Admin

18. Data Processors

18.1. Article 28 of the GDPR places a number of obligations on Data Processors. Security companies and other contractors that place, operate and / or monitor CCTV cameras on behalf of the Council are considered to be "Data Processors."

18.2. As Data Processors, they operate solely under the instructions of SDCC, as the data controller. They are only entitled to act on instruction from SDCC as the Data Controller. Where the Data Processor acts on their own instruction, this is considered a breach of contract and a personal data breach and is to be treated as such (See Section 22 below as concerns Personal Data Breaches).

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

18.4. Directors of Services/ Designated Staff Members must ensure that all security companies who process

data on behalf of the Council will be required to sign an appropriate Data Processing Agreement (DPA). The individual requirements on each Data Processing Agreement vary from contract to contract and are to be submitted to the DPO for approval as regards the requirements under the relevant Data Protection Legislation and this Policy, in advance of concluding the contract. The Data Processing Agreement must be submitted to the DPO as soon as it is renewed, changed, functions added etc. and the DPO is to be consulted prior to those amendments taking effect.

18.5. Directors of Services/ Designated Staff Members will ensure that the Data Processors are prepared to undergo an annual audit by the Designated Staff Member(s) and the DPO to ensure continued compliance with the applicable legislation and the Data Processing Agreement.

19. Data Subjects' Rights

19.1. Where CCTV recordings contain images of persons or personal identifiers, these images may be considered to be Personal Data and Data Subjects have the following statutory rights in relation to this data, which can be exercised at any time: a) Right to information, b) Right to complain to supervisory authority, c) Right of access, d) Right to rectification or erasure, e) Right to be forgotten, f) Right to restrict processing, g) Right to data portability, and h) Right to object and automated decision making/profiling.

19.2. For further information, please see our Data Protection Policy available at Privacy Statements - SDCC (https://www.sdcc.ie/en/services/our-council/access-to-information/privacy-statements/) or alternatively contact the Data Protection Officer at the contact details listed below.

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

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

20. Complaints

20.1. All data protection complaints with regard to all Council CCTV Systems must be directed to the Data Protection Officer in the first instance. dataprotection@sdublincoco.ie

20.2. The Data Protection Officer will retain a register of complaints..

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

In cases where the Council acts as a Joint Controller with An Garda Síochána, the joint controllership status will be communicated in the relevant privacy statement and the CCTV System Signage.

21.1. The Data controller is:
South Dublin County Council
County Hall Tallaght,
Dublin 24, D24 A3XC
Phone: +353 1 414 9000
Email: info@sdublincoco.ie

21.2. The Data Protection Officer for South Dublin County Council is:
Data Protection Officer
South Dublin County Council
County Hall Tallaght,
Dublin 24, D24 A3XC
Phone: +353 1 414 9000
Email: dataprotection@sdublincoco.ie

22. Communication, Implementation and Review

22.1. The Council will circulate this Policy to all staff and place it on the Intranet. It will also be published on the Council's website at www.sdcc.ie for the information of the public.

22.2. This Policy was approved by the County Council Senior Management Team and is issued on a version-controlled basis.

22.3. This Policy does not override any applicable national data privacy laws and regulations.

22.4. This Policy 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).

22.5. An evaluation of the implementation of this Policy 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.

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

23. Personal Data Breaches

23.1. As per the SDCC Personal Data Breach Policy, all personal data breaches arising from the processing of data through the use of CCTV Systems must be brought to the attention of the Council's Data Protection Officer immediately and without undue delay, along with a detailed report in relation to the breach.

24. Infringements of this Policy

24.1. Any act by a staff member in contravention of this Policy will be regarded as a disciplinary matter. South Dublin County Council reserves the right to take such action as it deems appropriate against staff members who violate any conditions of this Policy up to and including dismissal in accordance with the Local Authorities' Grievance and Disciplinary procedures. Staff are advised that serious breaches of this Policy may result in criminal or civil charges being brought against individuals.

Appendix I DPC CCTV Checklist

Directors of Service and Heads of Function are responsible for ensuring that any proposals in relation to the provision of new or existing CCTV scheme are in accordance with the terms of this Policy and take account of the following checklist issued by the Data Protection Commissioner in its CCTV Guidance Note, available on www.dataprotection.ie

CCTV Checklist from the Data Protection Commissioner

- **Purpose:** Do you have a clearly defined purpose for installing CCTV? What are you trying to observe taking place? Is the CCTV system to be used for security purposes only? If not, can you justify the other purposes? Will the use of the personal data collected by the CCTV be limited to that original purpose?
- **Lawfulness:** What is the legal basis for your use of CCTV? Is the legal basis you are relying on the most appropriate one?
- **Necessity:** Can you demonstrate that CCTV is necessary to achieve your goal? Have you considered other solutions that do not collect individuals' personal data by recording individuals' movements and actions on a continuous basis?
- **Proportionality**: If your CCTV system is to be used for purposes other than security, are you able to demonstrate that those other uses are proportionate? For example, staff monitoring in the workplace is highly intrusive and would need to be justified by reference to special circumstances. Monitoring for health and safety reasons would require evidence that the installation of a CCTV system was proportionate in light of health and safety issues that had arisen prior to the installation of the CCTV system. Will your CCTV recording be measured and reasonable in its impact on the people you record? Will you be recording customers, staff members, the public? Can you justify your use of CCTV in comparison to the effect it will have on other people? Are you able to Version Last Updated: October 2019 4 demonstrate that the serious step involved in installing a CCTV system that collects personal data on a continuous basis is justified? You may need to carry out a Data Protection Impact Assessment to adequately make these assessments.
- **Security**: What measures will you put in place to ensure that CCTV recordings are safe and secure, both technically and organisationally? Who will have access to CCTV recordings in your organisation and how will this be managed and recorded?
- **Retention:** How long will you retain recordings for, taking into account that they should be kept for no longer than is necessary for your original purpose?
- **Transparency**: How will you inform people that you are recording their images and provide them with other information required under transparency obligations? Have you considered how they can contact you for more information, or to request a copy of a recording?

This DPC CCTV checklist should be considered in advance of proposing the installation of CCTV Systems and provides guidance as to some of the key data protection considerations to be taken into account. The considerations outlined above are not exhaustive and are to be read in conjunction with this Policy and any other internal guidance provided by the Data Protection Officer and/or the Law Agent, as well as all applicable Codes of Practice/ guidance documents.

For Community CCTV Schemes, please additionally refer to the An Garda Síochána code of practice for Community based CCTV Systems. For all proposed CCTV Systems, please liaise with the Data Protection Officer prior to undertaking any of the above in order to receive an overview of the specific requirements for your proposed CCTV System.

Appendix II Data Subject Access Request Form

Connecting You to

Comhairle Contae Átha Cliath Theas
South Dublin County Council

Request for Access to Personal Data

(this includes CCTV and other Surveillance Technologies) under the Data Protection Act 2018 and under Article 15 of the General Data Protection Regulation 2016

This form is to be completed by the person requesting the access and submitted to dataprotection@sdublincoco.ie

Full Name: _____

Address: _____

_____

Email Address: _____
Please note that we will only use these details to process your request.

Where you (the data subject) make a request to access your personal data, the information shall be provided electronically via email or file share where possible, unless otherwise requested by the you.

Details of Request:
What Personal Data are you seeking access to?

_____

_____

_____

_____

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

Be as clear as possible about which details you are looking for, especially if you only want certain information. This will help the Council to respond more efficiently to your request.

Comhairle Contae Átha Cliath Theas, Halla an Contae, Lár an Baile, Tamhlacht, Átha Cliath 24.
South Dublin County Council, County Hall, Town Centre, Tallaght, Dublin 24.
Tel: +353 1 414 9000
SMS: 086 173 1707
Email: info@sdublincoco.ie
Ceangail 24/7 Connect 24/7 with Council information and services at www.southdublin.ie

Request For CCTV System Footage
If requesting access to CCTV & other Surveillance Technologies, please state the following:

Details of footage required: _____

_____

_____

Date: _____

Approximate Time: From: _____ To: _____

Location: _____

_____

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

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

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

_____

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

Print Name: _____

Signature: _____

Date: _____

Return to:
Dataprotection@sdublincoco.ie
Data Protection Officer
South Dublin County Council
County Hall Tallaght,
Dublin 24, D24 A3XC
Tel: +353 1 414 9000

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

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

Privacy Statement
South Dublin County Council processes all personal information in accordance with the General Data Protection Regulation 2016 and the Data Protection Acts, 1988 to 2018. The personal information (data) collected via this form is collected for the purpose of processing this application and any data collected is subject to the South Dublin County Council privacy statement which can be found at: https://www.sdcc.ie/en/services/our-council/access-to-information/data-protection/

Appendix III CCTV Download Request

Connecting You to

Comhairle Contae Átha Cliath Theas
South Dublin County Council

CCTV Footage Download Request Form

Please complete this form and submit it to dataprotection@sdublincoco.ie

Date: _____

Name: _____

Directorate & Section/Unit: _____

_____

Are you a CCTV Authorised Person: Yes / No

SDCC File Ref. No: _____

Urgency: (If the CCTV footage is set to delete within the next 48 hours, please mark your request as urgent)_____

Request: I wish to request approval to download CCTV footage required by South Dublin County Council under the following legislation for the following purposes.
Legislation: (Please cite the Irish legislation under which the CCTV footage is being sought)

_____

_____

Purposes(for which the footage is being downloaded, who is the recipient and what will they use the footage for etc.):

_____

_____

_____

Necessity & Proportionality Test: (The DPO can provide you with the legitimacy and necessity guidance)

_____

Comhairle Contae Átha Cliath Theas, Halla an Contae, Lar an Baile, Tamhlacht, Átha Cliath 24.
South Dublin County Council, County Hall, Town Centre, Tallaght, Dublin 24.
Tel: +353 1 414 9000
SMS: 086 173 1707
Email: info@sdublincoco.ie
Ceangail 24/7 Connect 24/7 with Council information and services at www.southdublin.ie

Details of the Footage being Requested.

Please include the following:
Details of footage required:

_____

_____

_____

_____

Date of footage: _____

(Approximate) Time: **From:** _____ **To:** _____

Location: _____

_____

APPROVED BY:

_____
(Data Protection Officer)

DATE: _____

Feeback/Comments:

_____

_____

APPROVED BY:

_____
(Senior Executive Officer)

DATE: _____

Appendix IV Access Log

The authorised access, downloading and/or viewing of CCTV System data is documented by the recording of the following in the access log for the CCTV System by the CCTV Authorised Person:

- CCTV Authorised Person processing the request;
- Date of request;
- Date request submitted to and acknowledged by Data Protection Office as well as DPO approval status;
- Description/reason for request, include all requirements as detailed under Section 16 of this Policy;
- Date and time footage is accessed and downloaded / removed from the system;
- Location of footage (camera reference/location);
- Response date and deadline (for data subject access request only);
- Search and review completed by - include third party/processor/staff name;
- Signature confirmation from both collecting official and official providing CCTV footage (signing logbook or confirmation letter);
- Confirmation that footage is provided via an encrypted device to the collecting official;
- The extent of information to which access was provided;
- The outcome, if any, of the viewing or download e.g. not of evidential value;
- The date the images were/ Will be subsequently deleted/ retained and the legal basis for such;
- The location of the retained footage.
- The access controls in place to protect the retained footage.

Appendix V Template Necessity and Proportionality Test

Template tailored for Necessity and Proportionality Test for Section 41 (b) DPA 2018 Requests

1. **Legitimate Aim**:
    a. Is the purpose of processing the personal data related to preventing, detecting, investigating, or prosecuting criminal offenses?
2. **Data Relevance:**
    a. Is the personal data being processed relevant to achieving the stated purpose or is it very broad and do you believe the scope could be narrowed?
    b. Are there less intrusive means to achieve the same objective?
3. **Lawful Basis:** In its Guidance on Legal Basis for Processing of December 2019, the Irish Data Protection Commission clarified that **the obligation to disclose personal data must derive from European Union law or Member State law and be one "to which the controller is actually subject".** As a result, a request from law enforcement that merely cites Section 41(b) **is not sufficient on its own** to oblige the data controller to disclose the data or records requested.
    a. Is there a clear and lawful basis for processing this data for the specified purpose?
4. **Special Category Data:**
    a. If special categories of personal data are being requested, is there a lawful basis for processing such sensitive information?
    b. Have AGS listed additional safeguards to protect this sensitive data? If not, ask them.
5. **Data Minimization:**
    a. Is the processing of personal data limited to what is strictly necessary to achieve the purpose of crime prevention and detection?
    b. Are excessive or irrelevant data avoided? i.e. Has the member of AGS confirmed that they are limiting the data to what is necessary and relevant and they have documented their analysis of such? If not, ask them!
6. **Duration of Processing:**
    a. Will personal data be retained only for as long as necessary to achieve the specified purpose?
7. **Data Security:**
    a. How will the data be shared?
    b. Are appropriate technical and organizational measures in place to protect the data from unauthorized access, disclosure, or loss? At a minimum data can only shared in encrypted form. It is your responsibility to ensure the security of the data in transit.
8. **Transparency:**
    a. Have data subjects been informed about the processing of their data for this purpose, including the legal basis, purposes, and retention periods via the SDCC privacy policy?
    b. Would they expect their data to be processed in this way?
9. **Data Subject Rights:**
    a. Are data subjects provided with the opportunity to exercise their rights under the Data Protection Act, such as the right to access, rectify, or erase their data?
10. **Data Protection Impact Assessment (DPIA):**
    a. Where the processing may result in a high risk to the rights and freedoms of the data subjects, confirm with AGS that they have conducted a DPIA to assess and mitigate the risks associated with processing this data?
11. **Proportionality:**

    a. Is the processing of personal data proportionate to the potential benefits and necessity of preventing and detecting criminal offenses? Are there less invasive methods that could achieve similar results?
12. **Accountability:** Are there mechanisms in place to demonstrate compliance with data protection regulations, including record-keeping and documentation?
13. **Review and Monitoring:** Is there a system for ongoing review and monitoring of the data processing activities to ensure continued necessity and proportionality?

This sample test aims to guide you in assessing whether the processing of personal data for the investigation, prevention, detection and prosecution of criminal offences complies with the principles of necessity and proportionality as outlined in Section 41(b) of the Data Protection Act.