



Tyrrelstown
community centre

TYRRELSTOWN COMMUNITY CENTRE CLG

CCTV Policy

Document Control

Document Ref:	TCC SOP002	Title:	Data Protection Policy
Version & Date:	1.0 30 th July 2019	Author:	SFE Data Policy Sub-group
Directorate:	Tyrrelstown Community Centre CLG Board of Directors	Approved by Management:	July 2019
Reviewed:		Change History	

Introduction

Fingal County Council has given a licence to Tyrrelstown Community Centre CLG to oversee the management and operation of the facility. Tyrrelstown Community Centre CLG engages a Facilities Management company to manage the day to day operations of the facility on their behalf.

Closed Circuit Television Systems (CCTV) both internal and external are installed in the Community Centre.

Tyrrelstown Community Centre CLG undertakes to operate its CCTV and undertakes to ensure that those who operate CCTV 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 Data Protection Act 2018 and Freedom of Information Acts and Section 38 of the Garda Síochána Act, 2005.

1. Personal Data

CCTV capture data, i.e., images of persons, which is their personal data. This confers rights on them under the Data Protection Acts. Importantly, Tyrrelstown Community Centre CLG has duties and obligations as the holder of personal data, as in these cases, and must ensure such data is handled and managed correctly.

This policy document addresses these issues and sets out clearly what Tyrrelstown Community Centre CLG, as Data Controller, and Centre Manager as Data Champion must do to protect personal data in relation to CCTV.

2. Private and Public CCTV Systems

Tyrrelstown Community Centre CLG operates a private CCTV system.

A Private CCTV system is owned and managed by the company on the premises. Such areas of coverage include meeting rooms, sports hall, dance studio, main corridors and carpark. While there may be some capture of persons passing by the front of such buildings and in the carpark this CCTV is considered to be private.

This CCTV policy applies to all the controls and standards as set out below.

3. Video Recordings

CCTV in this policy document refers only to video recording.

4. Purpose of Policy

The purpose of this policy is to regulate the use of Closed Circuit Television Systems and its associated technology in the monitoring of:

A: Internal and external environs of the Community Centre under the remit of Tyrrelstown Community Centre CLG.

B: The ongoing security of all Centre users and staff.

C: Public areas

D: Such other purposes as may arise from time to time

CCTV is installed to enhance the security of the Tyrrelstown Community Centre CLG as well as to create a mindfulness among occupants and visitors that a surveillance security system is in operation at all times. Specifically, such CCTV surveillance is intended for the purposes of:

- protecting the buildings and assets at all times.
- promoting the health and safety of staff, visitors and customers.
- prevention of bullying.
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism)
- supporting the Garda in a bid to deter and detect crime.
- assisting in identifying, apprehending and prosecuting offenders.
- in respect of the usage by staff of CCTVS to ensure persons interacting with staff are aware that their actions are being recorded.

5. Scope

This policy relates to the locating and use of CCTVs, their monitoring, recording, security, control and use of recorded material as well as setting out the way by which persons and others can seek to see images and to ensure that CCTVs are operated in a manner compatible with this policy.

6. General Principles

Tyrrelstown Community Centre CLG is responsible for the protection of the Community Centre, equipment and other plant as well as for authorised individuals, visitors and customers to the premises. Usage of CCTV contributes to compliance with the Safety, Health and Welfare at Work Act, 2005 and Data Protection Act 2018.

The use of CCTV will be conducted in a professional, ethical and legal manner within the terms of this policy and the law and all CCTV and associated equipment are required to be compliant with this policy.

Data obtained by CCTV may only be released when authorised by the Data

Controller or others as designated. Requests for CCTV recordings from An Garda Síochána or other law enforcement agencies will be facilitated subject to a proper audit trail and within the law.

CCTV monitoring will be conducted in a manner consistent with all existing policies adopted by Tyrrelstown Community Centre CLG including Equality & Diversity Policy, Child Protection Policy, Dignity at Work Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies and guidelines such as those issued by the Office of the Data Commissioner.

Video monitoring of public areas and within the Community Centre for security purposes is limited to uses that do not violate the individual's reasonable expectation to privacy. CCTV will not be located in areas where staff and the public would expect absolute privacy.

Recognisable images captured by CCTV systems are "personal data" and subject to the provisions of the all current Data Protection legislation including, EU GDPR and Data Protection Act 2018.

7. Justification for Use of CCTV

Article 5, Section 1 (c) of the EU GDPR 2016/679 requires that data is "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".

This means that Tyrrelstown Community Centre CLG must be able to justify the obtaining and use of personal data by means of a CCTV system. The following uses are considered to be justified -

- The use of CCTV to control the perimeter of the Community Centre 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.
- In other areas of the Community Centre where CCTV has been installed, e.g. hallways, stairwells, meeting rooms, dance studio etc., these are to prevent risk to security and / or health & safety of authorised individuals, clients and visitors.
- The purpose of CCTV in the public areas of the Community Centre is to enhance security and health and safety for all.

8. Locations of Cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy will not take place. Cameras placed 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.

9. CCTV Video Monitoring and Recording

CCTV video monitoring and recording may include the following:

- Protection of the property: The building's perimeters, entrances and exits, lobbies and corridors, special storage areas, meeting rooms etc.
- Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas
- Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms
- Criminal Investigations
- Investigations carried out by other agencies

10. Covert Surveillance

Where An Garda Síochána requests to carry out covert surveillance in the Community Centre, any request will be in writing and require the approval of the Data Controller.

11. Notification & Signage

The Community Centre will place this policy on its website for the information of the public.

Adequate CCTV signage will be placed at locations where CCTV camera(s) are sited, including at entrances to the Community Centre as well as advance notices indicating the use of CCTV. Signage may include the name and contact details of the Data Controller as well as the specific purpose(s) for which the CCTV camera is in place in each location and any other information as required. Appropriate locations for signage may include:

- entrances to premises, i.e. external doors and entrance gates
- reception areas
- at or close to internal cameras.

12. Storage & Retention

Article 5 Section 1 (e) of the EU GDPR 2016/679 states that data "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*" This policy provides for a maximum retention period of 35 days, except where a need is identified that requires that such

images / recordings are retained in relation to incidents / events. This time frame also complies with the guidelines issued by the Office of the Data Protection Commissioner.

The recordings will be stored in secure environments with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of The Data Champion.

13. Access

Unauthorised access to recordings, monitors etc. will not be permitted at any time. DVRs will be password protected. A log of access to DVR's etc. will be maintained. In relevant circumstances, CCTV footage may be accessed:

- By An Garda Síochána on request in writing when a crime or suspected crime has taken place and / or when it is suspected that illegal / anti-social behaviour is taking place at the premises.
- to other statutory bodies as deemed appropriate or
- to assist the Data Controller, or relevant designated / authorised persons in establishing facts in cases of unacceptable behaviour or
- to data subjects (or their legal representatives), pursuant to an access request under the Data Protection Acts, where the time, date and location of the recordings is furnished to Tyrrelstown Community Centre CLG or
- to individuals (or their legal representatives) subject to a Court Order
- Tyrrelstown Community Centre CLG insurers where it requires same in pursuit of a claim for damage done to the premises, or injury to individuals

14. Access Requests

Under the Data Protection Acts, on written request, any person whose image may have been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image / recording exists, i.e. has not been deleted and provided also that an exemption / prohibition does not apply to the release.

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

To exercise a right of access, a data subject must make an application in writing to the Data Champion using the Subject Access Request form. Access requests can be made subject to the following:

- A person should provide all the necessary information to assist Tyrrelstown Community Centre CLG in locating the CCTV recorded data, such as the date, time and location of the recording.
- If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be released by Tyrrelstown Community Centre CLG.
- In seeking such an image, it will be necessary for the requester to submit their own photograph in order to ensure that it matches with that on the CCTV.
- In giving a person a copy of their data, Tyrrelstown Community Centre CLG may do so on a storage device. However, if other identifiable persons cannot be obscured, data will not be released.

15. Responsibilities

The Data Controller (Tyrrelstown Community Centre CLG) will:

- Ensure that the use of CCTV is implemented in accordance with the policy set down by Tyrrelstown Community Centre CLG.
- Oversee and co-ordinate the use of CCTV for safety and security purposes within the premises.
- Ensure that all existing CCTV are evaluated for compliance with this policy
- Ensure that any new CCTV Systems installed are compliant with this policy and that Privacy Impact Assessments are undertaken where necessary
- Ensure that systems for access control, monitoring, recording and storage of CCTV by Tyrrelstown Community Centre CLG is consistent with the highest standards and protections
- Ensure that systems for the release of any information or recorded CCTV material stored comply with this policy
- Consider feedback / complaints regarding possible invasion of privacy or confidentiality due to the location of a CCTV camera or associated equipment

The Data Champion will:

- Ensure that the use of CCTV systems is implemented in accordance with this policy
- Co-ordinate the use of CCTV monitoring
- Ensure that the CCTV monitoring is conducted in line with this policy
- Ensure that any new CCTV Systems installed are compliant with this policy and undertake Privacy Impact Assessments where necessary

- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a record of access (e.g. an access log) of any material recorded or stored in the system
- Ensure that monitoring storage devices are not duplicated for release
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Provide a list of the CCTV cameras and the associated monitoring equipment and the capabilities of such equipment to the Data Controller
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. NOTE: [Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by An Garda Síochána].
- Report on feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment to the Data Controller
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the Community Centre and be mindful that no such infringement is likely to take place
- Co-operate with the Data Controller in reporting on the CCTV system in operation
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring storage devices are stored in a secure place with access by authorised personnel only
- Ensure that images recorded are stored for a period not longer than 35 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 Board of Directors.
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas

16. Implementation & Review

This policy will be reviewed and evaluated from annually. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, An Garda Síochána, audit units (internal and external), legislation and feedback from staff and others.

Implementation of and adherence to the policy to be monitored by the Data Controller.

APPENDIX I – DEFINITIONS.

Definitions of words / phrases used in relation to the protection of personal data and referred to in the text of the policy:

Access Request – This is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and / or Section 4 of the Data Protection Acts.

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism. It includes in this policy the recording of sound.

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Data Controller – The legal entity that controls the contents and use of personal data.

Data Processing - performing any operation or set of operations on data, including:

Obtaining, recording or keeping the data - Collecting, organising, storing, altering or adapting the data - Retrieving, consulting or using the data - Disclosing the data by transmitting, disseminating or otherwise making it available - Aligning, combining, blocking, erasing or destroying the data

Data Champion - a person who processes personal information on behalf of a data controller for example, this might mean an employee of an organisation to which the data controller out-sources work.

Data Subject – an individual who is the subject of personal data.

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller.

APPENDIX 2– CHECKSHEETS

Processing Images-Accessing and Removing Images

There are only limited circumstances when images may be removed and viewed. Copies of images can only be made by the Data Champion. (This form must be completed each time images are removed and viewed.

Please see the access and disclosure policy for further information.

Date and time of removal	
Name of person removing the image	
Reason for removal	
Crime incident number (if applicable)	
Location of the images	
Signature of the collecting official where appropriate	
Date and time images were returned to the system (if retained for evidential purposes)	
Where the images removed for viewing purposes? (If YES, please complete the additional sections)	
Name(s) of the person(s) viewing the images, (if this should include third parties, the name of the organisation to which the third party belongs).	
Reason for the viewing	
The outcome, if any, of the viewing	