

CCTV Policy

Policy Number	Policy Developed by	Date Developed
21 – Schedule 5	Áine Forde	13.05.2021
Version	Amendments	
3	Full Review	
Reviewed by		Review completed
Áine Forde		11.08.2025
CEO signature		Next Review Date
		11.08.2028

Mission Statement

Enable people with complex needs to experience the same rights as every other citizen and as equal members of the community.

Contents

1.0	Policy Statement:	3
2.0	Policy Purpose:	3
3.0	Policy Scope	3
4.0	Legislative & Regulatory Framework:	3
5.0	Lawful Basis for Processing	3
6.0	Data Protection Impact Assessment (DPIA)	3
7.0	Purposes of CCTV	4
8.0	Covert CCTV Use	4
9.0	Audio Recording	4
10.0	Roles & Responsibilities	4
11.0	CCTV System Description	4
12.0	Camera Locations	4
13.0	Signage & Privacy Notices	4
14.0	Image Quality & Maintenance	5
15.0	Retention & Storage	5
16.0	Access & Disclosure	5
17.0	Subject Rights	5
18.0	Third-Party Processors	5
19.0	Breach Management	5
20.0	Staff Training	6
21.0	Policy Review	6

1.0 Policy Statement:

- 1.1. Closed Circuit Television (CCTV) on Aurora premises are operated in compliance with the Data Protection Acts 1988 to 2018, GDPR 2018 and the guidance of the Data Protection Commission (DPC). Aurora is the Data Controller for CCTB footage collected on its premises. The Data Protection Officer can be contacted at aine.forde@aurorakilkenny.ie.

2.0 Policy Purpose:

- 2.1. The purpose of this policy is to outline the safeguards, responsibilities and controls governing the operation of and access to Aurora's CCTV systems and recorded images, ensuring compliance with data protection law and the protection of individual privacy.

3.0 Policy Scope

- 3.1. This policy applies to all employees involved in the operation of Aurora's CCTV systems and any external contractors or service providers acting as Data Processors on behalf of Aurora.
- 3.2. People supported by Aurora are informed via an easy read version of this policy of the purpose, location and existence of the CCTV system in place.

4.0 Legislative & Regulatory Framework:

- 4.1. Data Protection Acts 1988 – 2018
GDPR Regulations 2018 (EU 2016/679)
Data Protection Commission (DPC) Guidance on the Use of CCTV (2023)

5.0 Lawful Basis for Processing

CCTV processing is carried out under the lawful basis of Legitimate Interests (GDPR Article 6(1)(f)), namely:

- Protecting the safety and security of people supported, staff, visitors, and assets.
- Protecting buildings, vehicles, and property against theft, vandalism, and damage.
- Assisting in the prevention, detection, and investigation of crime.

A Legitimate Interests Assessment (LIA) has been completed and documented.

6.0 Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment has been conducted for Aurora's CCTV systems, in compliance with GDPR Article 35. This assessment is reviewed at least annually or when changes to

the CCTV system occur.

7.0 Purposes of CCTV

CCTV is used only for the purposes set out in section 5.0 and will not be used for any other purpose, such as employee monitoring, except in exceptional cases where covert surveillance is legally justified.

8.0 Covert CCTV Use

Covert CCTV surveillance is prohibited except where:

- It is authorised by senior management,
- It is strictly necessary for the investigation of suspected criminal activity, and
- It is carried out in consultation with An Garda Síochána.

9.0 Audio Recording

CCTV systems operated by Aurora do not record audio. If audio recording is introduced in the future, this policy will be updated and appropriate safeguards, consent, and lawful basis will be applied.

10.0 Roles & Responsibilities

The Head of Housing and Estates has overall responsibility for the CCTV system and oversight of third-party service providers.

Access to the system is restricted to authorised Health & Safety personnel and contracted maintenance providers, on a strict need-to-know basis.

All access is logged and subject to audit.

11.0 CCTV System Description

The CCTV system records 24/7, capturing images with motion detection, including date, time, and location metadata.

Footage is retained for a maximum of 28 days, unless required for an active investigation or legal proceedings.

All cameras are fixed-position; none are hidden without legal authorisation.

12.0 Camera Locations

Cameras are installed in strategic external and internal locations, primarily at entrances, exits, and other areas where security is necessary. Cameras are positioned to minimise unnecessary intrusion into private spaces.

13.0 Signage & Privacy Notices

Prominent CCTV signage is displayed, clearly stating:

- That CCTV is in operation,
- The purpose of CCTV,
- Aurora's contact details,
- Contact details for the DPO.

14.0 Image Quality & Maintenance

CCTV equipment is maintained to ensure image clarity sufficient for its stated purposes. Regular inspections are carried out, and faults are promptly repaired.

15.0 Retention & Storage

Footage is securely stored and protected using encryption and access controls. Any extended retention for evidential purposes is documented and justified.

16.0 Access & Disclosure

Access to images is restricted and documented.

Disclosure to third parties is only permitted in line with GDPR, the Data Protection Acts, and the following legal grounds:

- Court Order,
- Subject Access Request,
- Garda request for law enforcement purposes,
- Other statutory requirement.

17.0 Subject Rights

Individuals have the following rights under GDPR:

- Access to their personal data (Subject Access Request),
- Request erasure (where applicable),
- Request restriction of processing,
- Object to processing (where lawful basis is legitimate interests).

Requests must be made in writing to the DPO and will be responded to within one month, subject to lawful exemptions.

18.0 Third-Party Processors

All third parties with access to Aurora's CCTV data are bound by a written Data Processing Agreement (DPA) that meets GDPR Article 28 requirements.

19.0 Breach Management

Any suspected or actual personal data breach involving CCTV footage will be reported immediately to the DPO.

If required, the DPC will be notified within 72 hours in accordance with GDPR Article 33.

20.0 Staff Training

All relevant employees will receive induction and refresher training on this policy, data protection, and CCTV operational procedures.

21.0 Policy Review

This policy will be reviewed annually, or sooner if there are significant changes to legislation, technology, or operational use.