



Group CCTV Policy

1. Purpose

1.1 We use CCTV cameras to view and record individuals on or around our premises in order to maintain a safe environment for staff and visitors and for the other purposes described in this Policy. However, we recognise that the images and recordings of individuals recorded by CCTV cameras are Personal Data which must be processed in accordance with applicable data protection legislation. We are committed to complying with all applicable data protection legislation and ensuring that our CCTV systems are operated in accordance with the principles of fairness, lawfulness, transparency and accountability under the GDPR.

1.2 The purpose of this Policy is to:

- (a) outline how and why we will use CCTV and how we will process data recorded by CCTV cameras;
- (b) ensure that the legal rights of Data Subjects relating to their Personal Data are recognised and respected;
- (c) assist employees in complying with their own legal obligations when working with Personal Data;
- (d) explain how to make a subject access request in respect of Personal Data created by CCTV.

1.3 This Policy replaces and supersedes any and all previous policies that the Group may have in place insofar as they relate to CCTV and in the event of any conflict between the terms of this Policy and any other CCTV policy operated by any company or location within the Group, this Policy will prevail.

1.4 This Policy will be reviewed annually (or at such other times as the Group may determine) to ensure it is being applied as intended and may be adapted in light of any relevant changes in circumstances and/or to the extent necessary from time to time to comply with applicable laws.

2. Scope

2.1 This Policy relates directly to the use and purpose of CCTV and the monitoring, recording, access, requests and subsequent use of such recorded material or images. It applies to all directors, employees, contractors, third-party service providers, suppliers, visitors and guests of the Group and any other persons who interact with the Group's CCTV systems.

3. Data Controller

3.1 Under this Policy and unless the context otherwise requires in respect of any particular company or premises within the Group, Feldway Limited shall be the Data Controller. Feldway Limited has overall responsibility for the operation of this Policy.

4. Definitions

4.1 Under this Policy, the following expressions shall have the following meanings unless the context otherwise requires:

- (a) **CCTV:** Closed-circuit television, meaning a video surveillance system used to monitor and record activity in specific areas.
- (b) **Data Controller or Controller:** For the purposes of the GDPR and Data Protection Acts, the Data Controller will be Feldway Limited trading as The Fitzgerald Group, a company incorporated in Ireland under company number 250360 having its registered office at Palmerstown House, Dublin 20, Palmerstown, Dublin A45D625 and/or the relevant affiliate within the Group.
- (c) **Data Protection Acts:** Data Protection Acts 1988 – 2018, as may be amended from time to time.
- (d) **DPIA:** Data protection impact assessment, a formal process used to identify, assess, and mitigate risks to Data Subjects' privacy when processing Personal Data.
- (e) **Data Subject:** An identified or identifiable natural person as defined in Article 4 of the GDPR.
- (f) **Delivery Areas:** Designated zones within Group premises where goods are received or dispatched.
- (g) **Detailed Request:** A formal written application submitted to the Responsible Department specifying the need for access to recorded footage.
- (h) **DSAR:** Data Subject Access Request as permitted by Article 15(3) of GDPR.
- (i) **GDPR:** Regulation (EU) 2016/679 (General Data Protection Regulation), as may be amended from time to time.
- (j) **Group:** Feldway Limited, its subsidiaries, and affiliated companies.
- (k) **Personal Data:** Any information from which a living person is identified or could be identified.
- (l) **Real-Time Access:** The ability to view live CCTV footage as it is being recorded.
- (m) **Recorded Footage:** Video content that has been captured and stored by the CCTV system for later review.
- (n) **Responsible Department:** The designated internal team responsible for and authorised to oversee CCTV operations, access control, and footage review.
- (o) **Stocktaking Teams:** Employees or contractors responsible for inventory management and stock audits.

5. Lawful Purpose for Processing

5.1 Article 6 (1)(f) of the GDPR provides that processing must be necessary for legitimate interests pursued by the Data Controller or a third party, unless a Data Subject has an overriding interest in protecting their Personal Data.

- 5.2 Article 5(1)(c) of the GDPR requires that data is “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”.
- 5.3 Article 6(1)(c) of the GDPR also recognises that processing of Personal Data may be necessary for compliance with a legal obligation to which the Data Controller is subject and under Article 6(1)(d) of the GDPR processing of Personal Data may be necessary to protect the vital interests of Data Subject or other persons.
- 5.4 Prior to the installation or significant alteration of any CCTV system, a DPIA shall be conducted to assess the necessity and proportionality of processing and to mitigate privacy risks. A DPIA is intended to assist the Group in deciding whether new surveillance cameras are necessary and proportionate in the circumstances, whether they should be used at all, and/or whether any limitations should be placed on their use.
- 5.5 Any DPIA will consider the nature of the problem that the Group is seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, the Group will consider the effect a surveillance camera will have on Data Subjects and therefore whether its use is a proportionate response to the problem identified.
- 5.5 No surveillance cameras will be placed in areas where there is a legitimate expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by the Group to be necessary to deal with very serious concerns.
- 5.6 We obtain and use Personal Data by means of a CCTV system for the following reasons:
- (a) to protect the Group’s buildings, goods and assets, both during and outside operational hours;
 - (b) to prevent, detect and investigate crime or a potential crime, including vandalism of Group property, and to support the Gardai, law enforcement, and/or other relevant authorities in the prevention, detection, investigation and prosecution of crime;
 - (c) to investigate inappropriate behaviour or accidents, aid in disciplinary or other proceedings, and/or protect the integrity of the Group (for example in the event of alleged theft, fraud, discrimination, inappropriate operational procedures, bullying, or breach of Group policies) whether involving members of staff or the public;
 - (d) to ensure the health, safety and security of Data Subjects on Group premises;
 - (e) to assist with the data-to-day management of the Group, including assistance with stock taking, stock management and deliveries;
 - (f) to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings; and/or
 - (g) to assist in the defence of any civil litigation, including employment tribunal proceedings.
- This list is not exhaustive and other purposes may be or become relevant.
- 5.7 To satisfy these purposes of processing and/or to investigate an incident and/or to comply with applicable legislation and/or to the extent it is necessary and proportionate in the legitimate

interests of the Data Controller, CCTV images may be transferred by the Group (or the relevant Data Controller) via its Responsible Department or other authorized personnel to third parties. On occasion, we may be asked to disclose CCTV recordings to third parties for a purpose other than that for which they were originally obtained. This may arise, for example, where a request is received from An Garda Síochána or another law enforcement body to provide footage to assist in the investigation of a crime, which is described further below under Section 8.2(c).

6. Operation of System

- 6.1 The Group CCTV systems are maintained and can only be accessed by the Responsible Department and other authorised personnel.
- 6.2 Recorded Footage is password protected and the system is housed in a secure, locked office with restricted access.
- 6.4 All CCTV cameras operate twenty-four (24) hours a day, seven (7) days a week, except for periods of breakdown or necessary maintenance.
- 6.5 Cameras are positioned to monitor only the areas intended to be covered by the equipment and are in both internal and external areas of the Group premises.
- 6.6 CCTV signage will be displayed in prominent locations on the Group premises to alert Data Subjects that their image may be recorded. The signs will contain the name and contact details of the relevant Data Controller, as required by Section 71(2)(b) of the Data Protection Act 2018.
- 6.7 The CCTV system records digital images. The CCTV cameras capture movement detected in the area under surveillance together with data about time, date, and camera location.
- 6.8 The equipment and recording media are checked or “serviced” on a regular basis to ensure the quality of the images, camera, and recording function.
- 6.9 Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.
- 6.10 **Covert Monitoring.** We will not engage in covert monitoring or surveillance other than on an exceptional case-by-case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. In the event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the relevant Data Controller and the Responsible Department. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision. Only limited numbers of people will be involved in any covert monitoring. Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

7. Real-Time Access

7.1. Permitted Real-Time Access & Playback

Any temporary Real-Time Access granted to anyone outside of the Responsible Department must be logged, specifying the reason, duration of access, and the approving authority within the Group. For example, the following Real-Time Access shall be permitted from time to time:

- **Stocktaking Teams:** Real-Time Access and playback of CCTV feeds relevant to stockroom and inventory areas.
- **Delivery Areas & Playback:** Real-Time Access for operational oversight during active delivery windows.

7.2. Restricted Areas

All other areas are not accessible in real-time to any personnel outside the Responsible Department, other than in exceptional circumstances where it is considered appropriate and necessary and is authorised, for example to prevent imminent loss or damage to the Group.

8. Recorded Footage Access

8.1. Controlled Access

All access to Recorded Footage is strictly controlled by the Responsible Department.

8.2. Request Procedure

- (a) Requests for access to Recorded Footage must be submitted in writing by email to the Responsible Department at cctv@fitzgeraldgroup.ie.
- (b) Each request must include:
 - the reason for the request, in reasonable detail;
 - the specific date and time range requested;
 - the location to which the request relates; and
 - the authorising manager's name and contact details, where appropriate.
- (c) **An Garda Síochána:** Where the Group is required by law to provide Recorded Footage, this will be managed by the Responsible Department upon receipt of a valid request under Section 41(b) of the Data Protection Acts.
- (d) **DSAR:** Requests by Data Subjects to access Personal Data related to them, made under Article 15 of the GDPR, should be submitted in writing to the Responsible Department at cctv@fitzgeraldgroup.ie. Data Subjects should provide as much detail as possible to assist the Group (or the relevant Data Controller within the Group) in responding to their DSAR.

The following will be required:

- The request should be in writing and include reasonable details regarding the date, time and location of when and where the Data Subject reasonably thinks their image was recorded.
- Proof of identity, for example a copy of the Data Subject's passport or driver's license and proof of address.
- Any other particulars to identify the Data Subject on the Recorded Footage, for example a description of the clothing that was worn at the time in question or other details that may help us identify them in the footage.

All decisions taken by the Group in relation to DSAR's will be clearly communicated to the Data Subject.

If the Data Subject requests to view their own image on the Recorded Footage, the viewing will take place in a private office and will be facilitated by the Responsible Department, unless doing so is subject to a valid exemption, such as protecting the rights of other Data Subjects.

- (e) **Third Parties:** There may be instances where third parties, such as insurance companies, have a valid reason to request Real-Time Access or Recorded Footage. These requests will be reviewed on a case-by-case basis in accordance with the Data Protection Acts and the GDPR.

8.3. Review and Response

- (a) The Responsible Department will assess DSARs for validity and necessity.
- (b) Where validated and approved, a report will be compiled and shared with the requesting Data Subject. This report will include:
 - Summary of relevant footage;
 - Time-stamped observations;
 - Any anomalies or incidents noted.
- (c) Under Article 12(5) GDPR, in limited circumstances where a DSAR is “manifestly unfounded or excessive”, the Group may choose, in its reasonable discretion, to limit or deny access to the information requested.
- (d) The Group shall respond to DSARs without undue delay and in any event within one month from the date of receipt of a valid DSAR. That period may be extended by two further months where necessary, taking into account the complexity and number of requests.
- (e) Personal Data and other information related to others will be redacted and withheld and other restrictions or exemptions may apply.

9. Data Retention

Data recorded by the CCTV systems will be stored and will not be retained indefinitely. The retention period for CCTV footage will be for no longer than is necessary in accordance with the legitimate purposes of the processing but, in any case, no longer than thirty (30) days, save for in exceptional circumstances detailed below.

9.1. Extended Retention

Recorded Footage that is identified as relevant to an incident, investigation, or potential legal matter or where required otherwise by applicable law may be retained for longer periods, in accordance with applicable legislation.

9.2. Disposal

Recorded Footage that exceeds the retention period and is not flagged for extended retention will be automatically and securely deleted.

10. Complaints

- 10.1 Any complaints in relation to this Policy should be addressed to the Data Controller who can be contacted at data@fitzgeraldgroup.ie.
- 10.2 Complaints may also be made to the Data Protection Commission in Ireland.

Schedule 1 - Summary of Request Types.

Request Type	Requested By	Purpose
Recorded Footage Requests	Area Managers, Health & Safety Department, HR Department, General Managers, Legal or compliance officers Gardai, Insurance Co. All requests emailed to cctv@fitzgeraldgroup.ie	Investigating incidents or accidents to include disciplinary or other proceedings (for example, in the event of alleged theft, fraud, discrimination, or bullying), whether involving members of staff or the public. Providing evidence for insurance claims or legal proceedings, as outlined in this policy.
Playback Monitoring Requests	Stocktaking Team	Monitoring high-risk areas during peak hours or events, overseeing deliveries and/or stock movements.
Technical Support or Maintenance Requests	IT or Facilities departments, Site managers	Reporting camera malfunctions or blind spots, requesting system upgrades or repositioning, ensuring data storage and backup systems are functioning. Any third-party contractor engaged for CCTV maintenance or monitoring must be bound by a written data processing agreement in compliance with Article 28 GDPR.
Access Permission Requests	Department heads, External auditors or investigators (with authorisation)	Granting temporary or role-based access to specific camera feeds, supporting audits or compliance checks.
Reporting and Analytics Requests	Senior management, Risk and compliance teams	Reviewing trends in incidents or security breaches, assessing operational efficiency or compliance, informing policy updates or training needs.
DSAR	Data Subject	Access Request in line with Article 15 of the GDPR to be made to the cctv@fitzgeraldgroup.ie