

CCTV POLICY

Version:1.2 Revision Date: October 2027

CCTV Policy & Code of Practice

Grimsby Fish Dock Enterprises Ltd

Document owner	Andrew Oliver (CEO)
Approver	Board of Directors / Senior Management
Version	1.2
Effective date	14 th October 2026
Last reviewed	17 July 2026
Next review due	Within 12 months, or sooner if law, guidance, technology or operational use changes

Contents

Introduction.....	3
Purpose of CCTV System.....	3
Lawful Basis for Processing	3
Transparency & Signage.....	4
Scope of CCTV Coverage.....	4
Data Minimisation & Proportionality.....	4
Storage & Retention.....	5
Access to Footage	5
Data Subject Rights	5
Security Measures	6
Monitoring of Staff	6
Third-Party Processors	6
Review & Governance.....	6
Complaints.....	7
Accountability Statement.....	7

Introduction

Grimsby Fish Dock Enterprises Ltd ("GFDE") operates a CCTV system across its estate in order to protect people, property, and business operations.

This policy outlines how GFDE uses CCTV in compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025, where in force and applicable
- Information Commissioner's Office (ICO) guidance on CCTV and video surveillance
- Surveillance Camera Code of Practice as good-practice guidance, where applicable

GFDE recognises that CCTV images are personal data where individuals can be identified and therefore must be processed lawfully, fairly and transparently. GFDE will review this policy and associated CCTV procedures to reflect any applicable changes arising from the Data (Use and Access) Act 2025 and updated ICO guidance.

GFDE will maintain its registration with the Information Commissioner's Office and pay the data protection fee unless a valid exemption applies.

Purpose of CCTV System

GFDE operates CCTV for the following legitimate purposes:

- Prevention and detection of crime
- Public and staff safety
- Protection of assets, vessels, vehicles, and infrastructure
- Monitoring of restricted and high-risk operational areas
- Assisting law enforcement where required
- Supporting investigation of incidents, accidents, or breaches of site rules

CCTV will not be used for:

- Routine monitoring of staff performance
- Covert surveillance (unless legally authorised)
- Monitoring in private areas (e.g. toilets, changing rooms)

Lawful Basis for Processing

GFDE processes CCTV footage under:

Article 6(1)(f) UK GDPR – Legitimate Interests

Our legitimate interests include maintaining safety, preventing crime, and protecting critical port infrastructure.

A Legitimate Interests Assessment (LIA) has been conducted to ensure that:

- The use of CCTV is necessary
- It is proportionate
- Individuals' rights and freedoms are not overridden

Where CCTV captures employees, processing may also fall under:

- Article 6(1)(c) – Legal obligation (health & safety duties)

Transparency & Signage

GFDE ensures transparency by:

- Displaying clear, visible and readable CCTV signage at all entry points and relevant monitored areas before individuals enter areas where they may be recorded
- Identifying GFDE as the data controller
- Providing contact details for data protection enquiries
- Making this policy available upon request and via company website (if applicable)

Signage complies with ICO guidance and includes:

- The fact that CCTV is in operation
- The purpose of surveillance
- GFDE's identity as data controller
- Contact information for enquiries and requests

Scope of CCTV Coverage

Cameras are located in:

- Dock entrances and exits
- Quaysides and operational areas
- Warehouses and storage facilities
- Car parks
- Perimeter fencing and restricted zones

Cameras are positioned to:

- Focus on business premises and public safety areas
- Avoid unnecessary capture of neighbouring properties
- Minimise intrusion into private spaces

Audio recording is **not** routinely enabled unless justified and documented.

GFDE will maintain a CCTV camera register recording each camera's location, purpose, field of view, retention period, audio status, responsible owner and review date. The register will be updated when cameras are added, moved, removed or materially reconfigured.

Data Minimisation & Proportionality

GFDE ensures:

- Cameras are only installed where necessary
- Field of view is restricted to relevant areas
- Zoom and tracking functions are used proportionately
- Regular reviews assess continued necessity

A Data Protection Impact Assessment (DPIA) has been conducted due to the scale of monitoring in a public-access environment.

The DPIA and LIA will be retained with GFDE's data protection records, identify the approving person or body, and be reviewed when there is a material change to the CCTV system, its purpose, technology, coverage or risk profile.

Storage & Retention

- CCTV footage is stored securely on encrypted systems
- Access is password protected and restricted
- Footage is normally retained for **30 days** unless required for investigation, legal, regulatory, insurance or safeguarding purposes
- The retention period is based on operational need, risk and the purpose for which CCTV is used, and will be reviewed periodically
- Where footage is required for legal or insurance purposes, it will be retained only as long as necessary and access will remain restricted

Automatic deletion processes are in place to ensure compliance with the storage limitation principle.

Access to Footage

Access is strictly limited to:

- Authorised GFDE management
- Security personnel
- IT administrators (where technically necessary)

All access is:

- Logged and auditable
- Subject to strict confidentiality

Footage may be shared with:

- Police or law enforcement (with appropriate request)
- Insurance companies (where relevant)
- Legal representatives

All disclosures are documented.

Data Subject Rights

Individuals have rights under UK GDPR, including:

- Right of access (Subject Access Request – SAR)
- Right to erasure (where applicable)
- Right to restriction of processing
- Right to object

Subject Access Requests (SAR)

Requests may be made in writing or by any other clear method. To help GFDE locate the relevant footage, requesters should, where possible:

- Provide sufficient information to identify footage, such as date, time, location and description
- Provide proof of identity where reasonably required
- Explain any urgent reason for the request, if applicable

GFDE will respond within **one calendar month**.

Where third parties appear in footage:

- Images may be redacted
- Access may be partially restricted to protect others' rights

- GFDE may seek clarification where needed to locate footage or protect the rights of others

Security Measures

GFDE applies appropriate technical and organisational safeguards:

- Encrypted storage
- Firewall-protected networks
- Secure server rooms
- Role-based access controls
- Staff confidentiality agreements
- Regular password updates
- Annual system security review

Any data breach will be:

- Assessed immediately
- Reported to the ICO within 72 hours if required
- Communicated to affected individuals where high risk exists

Monitoring of Staff

CCTV is not used for continuous monitoring of employees.

Employees, contractors and regular site users will be informed about the nature, extent and reasons for CCTV monitoring, including through this policy, signage and relevant staff communications.

Where footage forms part of a disciplinary or incident investigation:

- It will be used fairly and proportionately
- Employees will be informed
- ACAS guidance will be followed

Third-Party Processors

Where external contractors maintain the CCTV system:

- A written Data Processing Agreement (DPA) is in place
- Processors must comply with UK GDPR
- Confidentiality and security standards are contractually enforced

GFDE remains responsible for ensuring processors provide sufficient guarantees for security, confidentiality, access control, deletion, audit support and assistance with data subject rights and breach reporting.

Review & Governance

GFDE will:

- Review this policy annually
- Reassess necessity of cameras periodically
- Conduct DPIA reviews when expanding the system
- Ensure staff training on data protection responsibilities
- Maintain evidence of ICO registration or exemption, DPIA/LIA records, signage checks, access logs, disclosure logs and the CCTV camera register

- Treat the Surveillance Camera Code of Practice as good-practice guidance unless GFDE is acting as, or on behalf of, a relevant authority to which the Code directly applies

Complaints

Individuals may contact:

Data Protection Lead

Grimsby Fish Dock Enterprises Ltd
Grimsby Fish Market
Wharnccliffe Road
Grimsby
NE Lincs
DN31 3QJ

Pete@grimsbyshipyardservices.com
07889141867

If unresolved, complaints may be made to:

Information Commissioner's Office (ICO)

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113

Website: www.ico.org.uk

GFDE will handle complaints promptly, fairly and in accordance with applicable data protection complaints requirements.

Accountability Statement

Grimsby Fish Dock Enterprises Ltd is committed to:

- Lawful, fair and transparent processing
- Data minimisation
- Storage limitation
- Integrity and confidentiality
- Demonstrable compliance

We recognise our responsibility to balance security needs with individual privacy rights and operate our CCTV system accordingly.

Annex A – Data Protection Impact Assessment (DPIA)

This DPIA records GFDE's assessment of the privacy risks arising from its CCTV system and the controls in place to ensure that CCTV use remains necessary, proportionate, lawful, fair and transparent.

DPIA field	GFDE record
Project / processing activity	Use of CCTV across the GFDE estate

Controller	Grimsby Fish Dock Enterprises Ltd
Responsible owner	Andrew Oliver, CEO / Data Protection Lead
Purpose of processing	Prevention and detection of crime; public, staff and contractor safety; protection of assets, vessels, vehicles and infrastructure; monitoring of restricted and high-risk operational areas; incident investigation; supporting lawful requests from law enforcement.
Categories of personal data	Images of identifiable individuals, vehicles, vessel movements and associated time/location data. Audio is not routinely recorded unless separately justified and documented.
Data subjects affected	Employees, contractors, tenants, visitors, fish market users, vehicle drivers, vessel crew, members of the public and law enforcement or emergency service personnel attending site.
Scale and context	CCTV is used across a public-access operational dock estate, including entrances, exits, quaysides, car parks, warehouses, storage areas, perimeter fencing and restricted operational zones.
Lawful basis	Article 6(1)(f) UK GDPR – legitimate interests. Article 6(1)(c) may also apply where processing is necessary to support legal obligations, including health and safety duties.
Necessity and proportionality	CCTV is used only where necessary for stated security, safety and operational purposes. Camera views are limited to relevant areas and reviewed periodically. CCTV is not used for routine staff performance monitoring.
Consultation	Relevant staff, contractors, security providers and management should be consulted where appropriate. Signage and policy availability provide transparency to site users.
Retention	Footage is normally retained for 30 days unless required for investigation, legal, regulatory, insurance or safeguarding purposes.

Access controls	Access is restricted to authorised GFDE management, security personnel and IT administrators where technically necessary. Access and disclosures are logged and auditable.
Security measures	Encrypted storage, password protection, role-based access controls, firewall-protected networks, secure server areas, confidentiality requirements and periodic security review.
International transfers	No international transfers are intended. Any future cloud or remote access arrangements must be assessed before implementation.
Residual risk rating	Medium, provided all controls in this policy and annex are implemented and reviewed.
Approval	To be completed: approver, role, date and signature.
Review trigger	Annual review, or earlier if cameras, coverage, technology, purposes, processors, retention or legal requirements change.

Annex B – Legitimate Interests Assessment (LIA)

This LIA records GFDE's assessment that its use of CCTV is justified under Article 6(1)(f) UK GDPR, subject to the safeguards set out in this policy.

LIA stage	Assessment
Legitimate interest pursued	GFDE has legitimate interests in preventing and detecting crime, protecting people, vessels, vehicles, buildings, infrastructure and stock, supporting site safety, managing restricted areas, and investigating incidents.
Why the processing is necessary	The dock estate includes public-access and high-risk operational areas. CCTV provides a proportionate means of deterring crime, responding to incidents, supporting safety and preserving evidence where incidents occur.
Alternatives considered	Physical patrols, lighting, barriers, access controls and signage are used or considered, but are not sufficient on their own to provide continuous coverage, evidential records or timely incident review.

Impact on individuals	Individuals may be recorded while entering, leaving or using GFDE premises. The impact is limited by visible signage, restricted camera fields of view, no routine audio recording, limited retention and controlled access.
Reasonable expectations	Individuals using a working dock, fish market, car park, warehouse or restricted operational area can reasonably expect proportionate CCTV for security, safety and operational protection, provided clear signage and policy information are available.
Safeguards	Clear signage, policy availability, camera register, DPIA review, access controls, disclosure logs, retention limits, security safeguards, SAR process, staff transparency and annual governance review.
Balancing outcome	GFDE's interests are not overridden by individuals' rights and freedoms, provided the safeguards in this policy and annex are maintained and CCTV is not used for routine staff performance monitoring or unjustified covert surveillance.
Decision	Proceed with CCTV processing under Article 6(1)(f), subject to annual review and review following material changes.
Approved by	To be completed: name, role, date and signature.

Annex C – CCTV Camera Register

This register must be maintained whenever cameras are installed, moved, removed, reconfigured or reviewed. Each camera entry should be checked at least annually.

Camera ID	Location	Purpose	Field of view	Audio?	Retention	Owner	Last reviewed	Action / notes
10.0.2.2	Auction Hall LHS Quay	Site security, vehicle access and incident review	Auction Hall	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)



10.0.2.3	Grading Machine 360	Site security, vehicle access and incident review	Grading Area	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.4	Quay side chiller Fast acting door	Site security, vehicle access and incident review	Grading Area	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.5	Auction Hall Adjacent Turnstile	Site security, vehicle access and incident review	Auction Hall	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.6	Manual Table 360	Site security, vehicle access and incident review	Grading Area	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.7	Grading Buyside	Site security, vehicle access and incident review	Grading Area	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.8	Grading Pallets	Site security, vehicle access and incident review	Grading Area	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)





10.0.2.9	Auction Hall	Site security, vehicle access and incident review	Auction Hall	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.10	Graveyard End	Site security, vehicle access and incident review	Outside	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.11	Auction Hall Bay	Site security, vehicle access and incident review	Auction Hall	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.12	Reception Area	Site security, vehicle access and incident review	Reception	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.13	Auction Hall	Site security, vehicle access and incident review	Auction Hall	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.14	Chiller 360	Site security, vehicle access and incident review	Chiller	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)





10.0.2.15	Loading Bay 2 180	Site security, vehicle access and incident review	Loading bays (Outside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.16	Loading Bay 6 180	Site security, vehicle access and incident review	Loading bays (Outside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.17	Loading Bay	Site security, vehicle access and incident review	Loading bays (Outside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.22	Rear Market Corner (OD)	Site security, vehicle access and incident review	Loading bays (Outside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.24	Loading Bay 10 180	Site security, vehicle access and incident review	Loading bays (Outside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.25	Loading Bay 12 180	Site security, vehicle access and incident review	Loading bays (Outside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)



10.0.2.40	Excel Shop Corner	Site security, vehicle access and incident review	Loading bays (Outside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.41	Excel Side Rear	Site security, vehicle access and incident review	Loading bays (Outside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.12	Excel Front Shop	Site security, vehicle access and incident review	Loading bays (Outside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.54	WC Corridor	Site security, vehicle access and incident review	Inside near reception	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.56	Roof Void Entrance	Site security, vehicle access and incident review	Inside roof void	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.58	New Market Entrance	Site security, vehicle access and incident review	Loading bays (Outside Dockside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)



10.0.2.64	Waste oil Bunker	Site security, vehicle access and incident review	Outside, Fuel Bunker	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.65	Sliding Gate (IN)	Site security, vehicle access and incident review	Outside	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.65	Sliding Gate (OUT)	Site security, vehicle access and incident review	Outside	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
10.0.2.67	Fuel Bunker Office End	Site security, vehicle access and incident review	Outside, Overlooking Bunker	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
	Quay North (PTZ)	Site security, vehicle access and incident review	Quayside (Dockside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
	Quay Mid (PTZ)	Site security, vehicle access and incident review	Quayside (Dockside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)





	Quay South (PTZ)	Site security, vehicle access and incident review	Quayside (Dockside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
	Graveyard (PTZ)	Site security, vehicle access and incident review	Quayside (Dockside)	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
	Main Entrance (Barriers PTZ)	Site security, vehicle access and incident review	Outside	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
	Quayside North (PTZ)	Site security, vehicle access and incident review	Overlooking Marine control / Carpark	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
	Office Entrance (PTZ)	Site security, vehicle access and incident review	Outside / Overlooking Carpark	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
	Canteen	Site security, vehicle access and incident review	Inside	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)



	Main Entrance Turnstile	Site security, vehicle access and incident review	Inside	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
	Main Office (PTZ)	Site security, vehicle access and incident review	Outside, Overlooking Carpark	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management D Payne	To be completed	Confirm signage visible before entry (Yes)
	Shipyard Office Wall	Site security, vehicle access and incident review	Office wall Outside	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management P. Brewster	To be completed	Confirm signage visible before entry. Yes
	Mess Room Wall	Site security, vehicle access and incident review	Outside Wall	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management P. Brewster	To be completed	Confirm signage visible before entry. Yes
	Outside Toilet Block Wall	Site security, vehicle access and incident review	Outside Overlooking Entrance	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management P. Brewster	To be completed	Confirm signage visible before entry. Yes
	Outside Toilet Block Wall	Site security, vehicle access and incident review	Outside Overlooking Entrance	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management P. Brewster	To be completed	Confirm signage visible before entry. Yes



	Container Roof (PTZ)	Site security, vehicle access and incident review	Overlooking Site	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management P. Brewster	To be completed	Confirm signage visible before entry. Yes
	Container Roof	Site security, vehicle access and incident review	Overlooking Site	No	30 days unless required for investigation or legal reason	Data Protection Lead / Site Management P. Brewster	To be completed	Confirm signage visible before entry. Yes

