Upper Medway Internal Drainage Board
CCTV Policy and Code of Practice

1. Introduction

This policy applies to overt CCTV at Board premises and operational sites, and to Board vehicle dashcams, wherever identifiable people are recorded. Its purposes are to protect staff, visitors, premises, vehicles and operational assets, and to provide evidence of relevant security or safety incidents. Surveillance must be necessary and proportionate to those purposes; this policy does not authorise general surveillance of the drainage district.

The Board must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended, including applicable amendments made by the Data (Use and Access) Act 2025. Personal data must be:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes and not further processed incompatibly with those purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Kept in identifiable form for no longer than necessary.
- Handled in a way that enables individuals to exercise their applicable rights.
- Protected by appropriate technical and organisational security measures.

The Board is responsible for, and must be able to demonstrate, compliance with the data protection principles (accountability).

2. Data Protection Statement

- Upper Medway Internal Drainage Board (the Board) is the data controller. The Clerk manages day-to-day operation and authorises access on the Board's behalf; this does not make individual staff separate data controllers.
- For surveillance necessary to support its statutory drainage and flood-risk management functions, the Board must document the public task basis under Article 6(1)(e) UK GDPR and the relevant legal powers, including under the Land Drainage Act 1991. Each system and purpose must have an assessed and recorded lawful basis; the Act does not itself authorise indiscriminate surveillance.
- The Board must not rely on legitimate interests when processing in performance of its public tasks. Any distinct activity outside those tasks requires a separately documented lawful basis and, where appropriate, a legitimate interests assessment. Consent is not the default basis for workplace or public-space surveillance.
- Before installing, materially changing or changing the purpose of a system, the Clerk must document necessity, proportionality, less intrusive alternatives and privacy risks, with advice from the Data Protection Officer (DPO). A data protection impact assessment (DPIA) must be completed where processing is likely to result in high risk, including systematic large-scale monitoring of publicly accessible areas. The Board will complete and maintain a DPIA for vehicle surveillance. Unmitigated high risks require prior consultation with the ICO.
- Cameras must minimise capture of neighbouring property, public areas and private activities, using positioning and privacy masking where appropriate. Staff must be informed and consulted about monitoring. Routine monitoring of staff productivity or movements is not authorised. Covert

surveillance is not authorised by this policy. Audio recording must be switched off by default; any exceptional use requires documented necessity, proportionality, a DPIA review and prior Board authorisation. Private vehicle use and out-of-hours recording must be addressed expressly in the assessment and staff information.

- Footage may be used in a specific staff investigation only where lawful, necessary, proportionate and consistent with the stated purposes or a separately assessed lawful use. Staff must be told about such potential use. This policy does not authorise facial recognition, biometric identification or automated disciplinary decisions; any proposed new use requires separate legal assessment and Board approval, including any applicable Article 9 or Article 10 safeguards.
- Clear signage must identify the Board, the surveillance purpose and a contact route, at premises and in or on vehicles as appropriate. A readily accessible CCTV privacy notice must explain the lawful basis, retention, recipients, individual rights, complaints route and DPO contact details. Staff must receive specific information about dashcam operation and any associated audio or location data.

As a public authority, the Board must appoint an independent, adequately resourced DPO, publish their contact details and notify the ICO. A Data Protection Lead is not a substitute for this statutory role. Any other duties must not create a conflict of interests. The Board retains responsibility for compliance. Surveillance must also respect Article 8 of the European Convention on Human Rights through the Human Rights Act 1998. The Board will use the Surveillance Camera Code of Practice as a governance benchmark and have due regard to it wherever legally required.

The Clerk must maintain a system register, processing records, lawful-basis assessments, DPIAs, retention schedules, access and disclosure logs, staff training records and processor agreements. Review this policy and the continuing necessity and proportionality of each system at least annually and after material changes or incidents, taking DPO advice. Before approval, verify actual camera coverage, dashcam recording modes and retention, signage, the published privacy notice, DPO arrangements, security and retrieval/redaction capability. Policy wording alone does not demonstrate operational compliance. Requests for information that are not subject access must be assessed under the Freedom of Information Act 2000 or Environmental Information Regulations 2004 as applicable, with the relevant personal-data protections; this policy must not be used to impose a blanket refusal.

3. Retention of Images

Recordings are stored on an onboard drive. The stated dashcam configuration is a 144-hour rolling recording, after which footage is overwritten cyclically. The Clerk must verify and document actual retention for each fixed or vehicle system, including whether this means recording hours or elapsed time. Retention must be justified by the specific purpose, not storage capacity; 144 hours is not a statutory retention period. Unnecessary footage must be securely overwritten or deleted.

Dashcams use the vehicle battery as their power supply. The Clerk must document when each system records, including parking mode, and test recording, timestamps, retrieval and secure deletion. Relevant footage must be promptly protected from routine overwriting once an incident, access request, complaint or legal hold requires preservation. Retained extracts must have a recorded reason, restricted access and a review/deletion date; they must be securely deleted when no longer needed.

4. Access to Images

It is important that access to, and disclosure of, images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes.

5. Access to Images by Staff

Access is limited to trained personnel authorised in writing by the Clerk on the Board's behalf, with DPO advice where appropriate. Board membership or employment alone gives no right of access. Requests by individuals and third parties must be assessed under the procedures below.

Viewing of images must be documented as follows:

- The name of the person removing from secure storage, or otherwise accessing, the recordings.
- The date and time of removal of the recordings.
- The name(s) of the person(s) viewing the images (including the names and organisations of any third parties).
- The reason for the viewing.
- The outcome, if any, of the viewing.
- The date and time of replacement of the recordings.

Recording equipment and removable media must be protected against theft and unauthorised access. Use individual accounts, appropriate authentication, access logs, maintained security updates, and encryption or equivalent risk-appropriate safeguards for stored and transferred footage. Viewing must take place privately; copying to personal devices or unauthorised online sharing is prohibited. Logs must identify the footage, authorisation, recipients and any copies or exports so that evidential integrity and the chain of custody can be demonstrated.

Loss, unauthorised viewing, disclosure or other suspected personal data breaches must be reported immediately to the Clerk and DPO under the Board's breach procedure. All breaches must be recorded and risk-assessed. The Board must notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to risk individuals' rights and freedoms, and inform affected individuals without undue delay where the risk is high.

6. Removal of Images for Use in Legal Proceedings

In cases where recordings are removed from secure storage for use in legal proceedings, the following must be documented:

- The name of the person removing from secure storage, or otherwise accessing, the recordings.
- The date and time of removal of the recordings.
- The reason for removal.
- Specific authorisation of removal and provision to a third party.
- Any crime incident number to which the images may be relevant.
- The place to which the recordings will be taken.
- The signature of the collecting police officer, where appropriate.
- The date and time of replacement into secure storage of the recordings.

7. Access to Images by Third Parties

Third-party requests should be recorded using the Application for CCTV Data Access form at **Appendix A**, or equivalent recorded information. The form is not compulsory for subject access requests.

The Clerk, acting for the Board and taking DPO advice where needed, must verify the requester's identity and authority, establish the purpose and lawful basis for disclosure, and document necessity, proportionality and authorisation. A request from the police, an insurer or a legal representative does not automatically entitle them to footage. Disclose only the necessary material by secure means and record the recipient, footage, date, purpose and legal justification. Potential recipients, subject to those checks, include:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry.

- Prosecution agencies.
- Relevant legal representatives.
    - The press or media only exceptionally, following the safeguards in section 8; a request for public assistance does not by itself justify disclosure.
    - Individuals requesting their own personal data, under sections 9 and 10. Any crime-related restriction must satisfy the applicable statutory exemption on a case-by-case basis; the existence of an investigation alone is not sufficient.

All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented as above.

8. Disclosure of Images to the Media

Media or public release is exceptional and requires prior written authorisation by the Clerk on the Board's behalf, with DPO advice and a documented lawful basis, necessity, proportionality and consideration of harm, victims' wishes and any police investigation. There must be no routine publication or social-media release of identifiable footage. Uninvolved individuals must be effectively masked or blurred where required; redaction alone does not make an otherwise unlawful disclosure lawful. If specialist editing is needed, the Board must use an approved processor with a binding written agreement meeting Article 28 UK GDPR, including:

- Documented instructions, confidentiality and appropriate security, including secure transfer and no independent use of footage.
- Prior authorisation of sub-processors, assistance with individual rights, security breaches and DPIAs, and lawful safeguards for any restricted international transfers.
- Return or secure deletion of footage at the Board's choice when services end, provision of compliance information and audit rights, and notification of unlawful instructions. The agreement must specify the processing purpose, duration, data and people concerned and the Board's rights and obligations.

9. Access by Data Subjects

Individuals have a right of access to their personal data under Article 15 UK GDPR. Requests may be verbal or written and made to any part of the Board; no legal wording or mandatory form is required. **Appendix A** is an optional aid. A reason for requesting personal data is not required. Seek only information reasonably needed to locate footage and verify identity or representative authority, such as approximate date, time, location and description. Do not routinely require photographs or identity documents where identity is already established. A copy of personal data and the required supplementary information must normally be supplied free of charge, securely and in an accessible format; viewing only is an option if the requester agrees.

10. Procedures for Dealing with an Access Request

All staff must recognise and promptly record access requests and refer them to the Clerk/Data Protection Lead, with DPO oversight and advice. The receipt date is the date any part of the Board receives the request. The Clerk must promptly identify relevant systems, make a reasonable and proportionate search, and preserve relevant footage before automatic overwriting.
Disclosure decisions remain the Board's responsibility. Insurer or legal advice may be sought where appropriate but is not a precondition for compliance and must not delay the statutory response. Consider third-party rights case by case, including consent or whether disclosure without consent is reasonable, confidentiality and the ability to redact rather than withhold the requester's data.

Where necessary, third-party images or audio must be effectively redacted, masked or blurred, while supplying as much of the requester's personal data as can lawfully be provided. Any editing provider must meet the full Article 28 processor requirements in section 8, including:

- Documented instructions, confidentiality and appropriate security for handling and transferring footage.
- Authorised sub-processors and assistance with rights requests, breaches and DPIAs, with any required international transfer safeguards.
- Defined processing details, return or deletion, compliance information and audit rights, as set out in section 8.

The Board must respond without undue delay and normally within **one calendar month**, not 30 days. Where reasonably necessary, identity or representative-authority evidence must be requested promptly and the statutory period calculated under the applicable rules. An extension of up to two further months is permitted where necessary because of complexity or the number of requests; the requester must be notified, with reasons, within the initial month. Any clarification-related pause may be used only where legally permitted and must be explained and recorded; requests for unnecessary information must not be used to delay access.

Retain a proportionate record of the request, receipt date, searches, identity checks, any lawful pause or extension, disclosure and response under a documented retention schedule. Any refusal, restriction or fee must have a specific lawful justification. Explain the decision and applicable reasons, and inform the requester of the Board's complaints route, their right to complain to the ICO and their right to seek a judicial remedy. Requests for erasure, restriction or objection must also be referred promptly to the Clerk and DPO and considered under the applicable UK GDPR provisions.

11. Complaints

Data protection complaints may be made verbally or in writing to the Clerk or DPO, including electronically; use of a particular form or channel is not compulsory. The Board must make the complaints route clear in its privacy information and provide reasonable assistance. Representatives must provide appropriate evidence of authority where needed, but a signed consent form is not the only possible evidence. Complaints will be acknowledged within seven days (and in all cases within the statutory 30-day limit). The Board must investigate appropriately, keep the complainant informed and communicate the outcome without undue delay. It aims to issue a written outcome within 21 days; where this is not possible it must explain why and give progress updates. Record the complaint, enquiries, outcome and any remedial action. Explain how the complainant may raise concerns with the ICO and seek a judicial remedy.

Oliver Pantrey
Clerk
10/11/26

Amendments March 2022

- Removed Lower Medway IDB References
- Removed plural use when referring to the Board
- Changed CEO to Clerk

Amendments November 2025

- Updated policy to reflect current CCTV usage within the company.

Amendments November 2026

- Updated the legal framework to UK GDPR and the Data Protection Act 2018 as amended, including applicable Data (Use and Access) Act 2025 changes; clarified the Board's controller responsibilities, public-task lawful basis and independent DPO requirements.
- Added necessity, proportionality, DPIA, privacy-notice and dashcam safeguards, including limits on staff monitoring and audio recording and consideration of public-authority privacy duties.
- Strengthened purpose-based retention, preservation of incident and requested footage, authorised access, secure handling, evidential integrity and personal data breach reporting.
- Tightened third-party and media disclosure controls and Article 28 requirements for editing and other processors.
- Corrected subject access procedures and Appendix A: optional form, no compulsory reasons, proportionate identity checks, reasonable and proportionate searches, normally free copies and a one-calendar-month response period with only lawful pauses or extensions.
- Updated data protection complaints handling for the Data (Use and Access) Act 2025 and added annual operational compliance checks and appropriate FOI/EIR request handling.

Appendix A

UK GDPR/Data Protection Act 2018 – Application for CCTV Data Access

This form is optional for subject access requests. Complete only the details reasonably needed to identify you, locate the footage and reply securely. Attach a separate sheet if helpful.

Applicant's name and contact details for a secure reply (a postal address is needed only where relevant)	
Name of the person whose personal data is requested, if different from the applicant	
If acting for another person, provide appropriate evidence of your authority, such as signed written authority. Other valid evidence will be considered.	Data subject's authority/signature, if applicable:
If signed authority is unavailable, explain your authority to act and provide appropriate supporting evidence	
Purpose and legal authority for third-party disclosure requests. For a request for your own personal data, reasons are not required.	
Date or approximate date range of the footage requested	
Time or approximate time range of the footage requested	
Location, site or vehicle, and camera if known	
Description sufficient to identify the person in the footage, such as clothing. Provide photographs or identity evidence only where reasonably necessary; do not send excessive personal information.	
Preferred secure delivery method. A copy will normally be provided; viewing only may be arranged if you agree.	

Subject access requests are normally free of charge. The Board will respond without undue delay and normally within one calendar month, subject only to the lawful identity, authority, clarification and extension rules explained in section 10. Completion of this form is not a condition of access.

INTERNAL USE ONLY	**INTERNAL USE ONLY**
Access granted (tick)	
Access **not** granted (tick)	Reason for not granting access:

Data Controller's details:	Name: Signature: ……. Date: