Upper Medway Internal Drainage Board
Data Retention and Disposal Policy

1. Introduction

1.1 This policy supports the Board's Data Protection Policy and governs compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR). It supports the Board's functions under the Land Drainage Act 1991 and its applicable accounts and audit obligations in England.

1.2 The Board must retain records needed for its statutory functions, accountability and legal obligations, and dispose of them when no longer required. Appendix A sets statutory minimums where applicable and Board retention and review rules elsewhere; it is not a statement that every period is prescribed by law. This policy must be reviewed annually and when legislation, guidance or Board activities change.

1.3 The organisation will ensure that information is not kept for longer than is necessary and will retain the minimum amount of information that it requires to carry out its functions and the provision of services, whilst adhering to any legal or statutory requirements.

2. Aims and Objectives

2.1 It is recognised that up to date, reliable and accurate information is a vital to support the work that the organisation does and the services that it provides to the area. This document will help us to:

- Ensure the retention and availability of the minimum amount of relevant information that is necessary for the organisation to operate and provide services to the area.
- Comply with FOIA, EIR, the UK GDPR and the Data Protection Act 2018 as amended, and applicable statutory requirements for the Board's drainage, financial and employment records.
- Save employees' time and effort when retrieving information by reducing the amount of information that may be held unnecessarily. This will assist them as they carry out their daily duties, or if searching for information requested under the Freedom of Information Act.
- Ensure archival records that are of historical value are appropriately retained for the benefit of future generations.

3. Scope

3.1 This policy applies to Board members, employees, contractors and others handling Board records. It covers paper and electronic records wherever held, including email, messages, shared and cloud storage, mobile devices, recordings, backups and records held by service providers on the Board's behalf.

3.2 Maintain an authoritative record and necessary audit trail. Retain original deeds, sealed documents and other originals where legal or evidential requirements require them; other paper records may be securely digitised after checking completeness, legibility and authenticity. Duplicate working copies must not be retained unnecessarily.

4. Standards

4.1 The Board must apply the following records-management standards:

- Apply the retention and review rules in Appendix A, recording the purpose, legal or business justification, responsible officer, start event and final action for each record category.
- Keep paper personal information in secure, locked storage with access restricted to authorised personnel. Keep electronic personal information in approved systems with role-based access, suitable authentication, security controls and protected backups.
- Keep DBS certificate information separately from general personnel records, with access restricted to those authorised to receive it for their duties.
- Appropriately dispose of information that is no longer required.
- Appropriate measures will be taken to ensure that confidential and sensitive information is securely destroyed.
- Long-term statistics should use genuinely anonymised information wherever possible. Pseudonymised information remains personal data. Identifiable records may be retained for public-interest archiving, research or statistics only where the applicable legal conditions and safeguards are met and documented.
- Maintain only necessary copies of personal information. Apply the same retention controls to email, downloads, shared storage and provider-held copies, and document any necessary differences for backups.

5. Breach of Policy and Standards

5.1 Any employee who knowingly or recklessly contravenes any instruction contained in, or following from, this Policy and Standards may, depending on the circumstances of the case, have disciplinary action, which could include dismissal, taken against them.

6. Roles and Responsibilities

6.1 Upper Medway Internal Drainage Board is the data controller. The Clerk is the policy owner and is accountable to the Board for its implementation; the Data Protection Officer provides independent advice and monitoring.

6.2 The Clerk must maintain the retention schedule and records inventory, allocate record owners, arrange staff training and documented disposal reviews, and check compliance at least annually with advice from the Data Protection Officer and relevant professional advisers.

6.3 Other delegated staff are responsible for ensuring their records are kept and destroyed in line with this policy.

6.4 The Clerk must authorise disposal or documented retention exceptions, confirm that no preservation hold applies, and ensure that the disposal method reflects the information's sensitivity. A disposal register must identify the record category and date range, authority, date, method and responsible officer, without reproducing unnecessary personal data.

6.5 Publish or otherwise provide clear retention periods or criteria in relevant privacy information. Staff must promptly refer requests for access, erasure, restriction or objections to the Clerk and Data Protection Officer for lawful assessment; retention requirements and exceptions must be considered, not assumed to override individual rights.

6.6 The Board must provide an accessible route for data protection complaints, including complaints about retention or disposal, acknowledge them within 30 days, investigate and keep the complainant informed, and communicate the outcome without undue delay. Record complaints and corrective actions under an approved, justified retention rule; explain the right to complain to the Information Commissioner.

7. Confidential Waste

7.1 Whether information is disclosable under FOIA or EIR is separate from the security required for its disposal. Public availability does not by itself make personal, sensitive or security-related information suitable for ordinary waste.

7.2 Personal data, confidential information and records whose disclosure could harm individuals, the Board or its operational security must be disposed of securely. Apply FOIA exemptions and EIR exceptions when deciding disclosure; a confidentiality label alone does not determine access rights.

7.3 Examples of what constitutes confidential waste:

- Exempt information contained within committee reports.
- Files containing the personal details of an individual and files that predominantly relate to a particular individual or their circumstances. For example, completed application forms and letters.
- Materials given to us on a 'confidential' or on a limited use basis e.g., material provided by contractors or the police.

7.4 Examples of what does not constitute confidential waste:

- Publications containing no personal, confidential or security-sensitive information may be recycled after checking that no retention requirement or preservation hold applies.
- Public committee reports and background papers may be recycled only where the particular copy contains no information requiring secure disposal, including annotations, attachments or unredacted personal details.

8. Disposal of Documentation

8.1 Securely destroy confidential paper records by effective shredding or an approved confidential-waste service, with locked storage pending destruction. For external destruction obtain evidence

of secure disposal and appropriate contractual safeguards. Ordinary recycling must not be used for personal or confidential records.

8.2 Apply secure deletion to electronic records, email, recordings, cloud copies and storage media, including provider-held data. Before reusing or disposing of equipment, securely sanitise or destroy media. Where backup data cannot immediately be selectively erased, put it beyond operational use until overwrite under a documented, justified backup cycle; reapply deletions before restored data is returned to use. Document provider deletion arrangements and verify completion.

8.3 Suspend routine deletion, including automatic expiry, when records are relevant to an information or data-subject request, complaint, audit, investigation, litigation or reasonably anticipated claim. Preserve relevant records through reviews, appeals and any applicable inquiry hold; the Clerk must document scope, notify staff and providers, review necessity and authorise release. Records must never be altered, concealed or destroyed to prevent lawful disclosure, including under section 77 FOIA or regulation 19 EIR.

9. Retention

9.1 Retention periods reflect applicable legislation, regulatory guidance and documented Board business needs. Professional guidance is not itself a statutory retention rule. Retain personal data only for as long as necessary for a lawful purpose, subject to applicable statutory minimums and preservation holds.

9.2 Throughout retention the conditions regarding safe storage and controlled access will remain in place.

9.3 DBS certificate information must be kept securely, separately from personnel files, with access limited to authorised recipients. It is criminal-offence data: record the Article 6 lawful basis and the Article 10 authority or applicable Data Protection Act 2018 Schedule 1 condition, with an appropriate policy document where required.

9.4 Retain DBS certificate information only as long as necessary after the recruitment or other relevant decision, normally no longer than six months as the Board's default. Any exceptional extension requires a recorded necessity, lawful basis and review date, with Data Protection Officer advice. Securely destroy certificates, images and representations of their contents when no longer needed. A limited check record may retain the issue date, subject's name, check type, position, certificate reference and recruitment decision for the justified personnel-record period; it must not reproduce conviction details.

9.5 Any unauthorised employee accessing or attempting to access Disclosures or Disclosure information, or personnel records will be dealt with under the organisation's disciplinary procedures.

9.6 Appendix A governs review and disposal. Record owners must apply its start events and distinguish legal minimums from Board policy periods. At expiry, delete or anonymise records unless a documented legal obligation, preservation hold or justified continuing purpose requires

retention. Record the reason, scope, authorisation and next review date for any extension; discretion is not permission for indefinite retention.

10. Storage and Access

10.1 DBS certificate information must be held separately from personnel files in secure, lockable, non-portable storage or an approved electronic system with equivalent access restrictions. Access is limited to the Clerk and expressly authorised personnel who need it for their duties.

11. Handling

11.1 The organisation complies with s124 of the Police Act 1997, so that Disclosure Information is only passed to those who are authorised to receive it in the course of their duties. The organisation maintains a record of all those to who Disclosures or Disclosure Information has been revealed and recognises that it is a criminal offence to pass this information to anyone who is not entitled to receive it.

11.2 Personal information will only be available to those who are authorised officers.

11.3 Data and information will be kept up to date and reviewed annually by an authorised officer.

12. Usage

12.1 DBS certificate information may be used only for the specified, lawful recruitment or other relevant purpose for which it was obtained. Obtain the applicant's permission where required by the DBS process; that permission does not replace the need to identify a lawful basis and criminal-offence-data condition. Internal sharing is limited to authorised recipients with a necessary role in that purpose.

12.2 Explain to the individual the purposes and authorised recipients or recipient categories through appropriate privacy information, subject to any lawful restriction. General internal sharing of DBS certificate information is not permitted.

APPENDIX A

Recommended Document Retention Timescales.

Financial records expressed simply as a number of years are retained for that period after the end of the relevant financial year. For all other records, use the stated event (for example creation, decision, expiry, closure, disposal or end of employment); where none is specified, count from closure of the record or case. Do not add the current financial year to periods stated in months, days or from a specific event. Statutory minimums take precedence. Board policy periods are review and disposal rules, not automatic authority to retain unnecessary personal data.

This schedule is not exhaustive. The Clerk must assign a documented purpose, lawful basis, responsible officer, start event, review date and disposal or archival action to any unlisted category before routine retention is authorised. "Indefinitely" means selected for permanent corporate or public-interest archival preservation, not unrestricted retention of every copy or personal detail. Review personal information and restrict, redact or anonymise it where appropriate. Generic entries apply only where the Board actually holds those records for a lawful function.

Document Retention Period

Finance

Document	**Retention Period**
Financial Published Final Accounts	Indefinitely
Signed Audited Accounts	Indefinitely
Final Account working papers	7 years
Records of all accounting transactions held by the Financial Management System	At least 7 years
Cash Books (records of monies paid out and received)	7 years
Purchase Orders	7 years
Cheque Payment Listings (Invoices received)	7 years
Payment Vouchers Capital and Revenue (copy invoices)	7 years
BACS listings	7 years
Goods received notes, advice notes and delivery notes	7 years
Copy receipts	7 years
Petty cash vouchers and reimbursement claims	7 years
Debtors and rechargeable works records	7 years
Expenses and travel allowance claims	7 years
Asset Register for statutory accounting purposes	7 years
Journal Sheets	7 years
Ledger / Trial Balance	7 years
Year end ledger tabulations – ledger details and cost updates	7 years
Published Budget Books	Indefinitely (published corporate record)
Financial Plan	Indefinitely
Budget Estimates – Detailed Working Papers and summaries	7 years

Bank Statement (Disk Space) and Instructions to banks	7 years
Bank Statements (Hardcopy)	7 years
Banking Records including Giro cheques, bills of exchange and other negotiable instruments	7 years
Prime evidence that money has been banked	7 years
Refer to Drawer (RD) cheques	7 years
Cancelled Expenditure cheques	7 years
Bank Reconciliation	7 years
Cheques presented / drawn on the bank accounts	7 years
Prime records that money has been correctly recorded in the organisations financial systems	7 years
Grant/Funding Applications & Claims	7 years
Precept Forms	Indefinitely
Internal Audit Plans/ Reports	7 years
Fees and Charges Schedules	7 years
Time sheets and overtime claims	7 years
Payroll and tax information relating to employees	7 years
Payroll costing analysis	7 years
Records of payment made to employees for salaries / wages (including intermediate payslips)	7 years
Statutory end of year returns to Inland Revenue and Pensions Section	Board policy: 7 years after the relevant tax year for tax returns; pension entitlement and service evidence retained for as long as needed to administer or establish pension rights, with a documented review rule and restricted access.
Loans and Investment Records; temporary loan receipts and loan tabulations	7 years (after redemption of loan)
VAT, Income Tax and National Insurance Records	7 years
Current and expired insurance policies, schedules and evidence of cover	Retain for the period needed to evidence cover and resolve potential liabilities, including long-tail employer liability claims. Clerk to record insurer/legal advice and review dates; do not apply a blanket 7-year disposal rule to evidence of cover.
Insurance claim files (separate from evidence of cover)	Board policy: 7 years after final settlement or closure; extend where insurer/legal advice, long-tail liability or a preservation hold requires it.
Capital and contracts register	Indefinitely
Final accounts of contracts executed under hand	7 years from completion of contract

Final accounts of contracts executed under seal	Board policy: 12 years after completion or termination, and longer where needed to cover the applicable limitation period from accrual of a cause of action or a preservation hold. Review with legal advice; section 8 Limitation Act 1980 concerns actions on specialties, not a universal destruction date.
All Other reconciliations	7 years

Personnel

Unsuccessful application forms	6 months
Unsuccessful reference requests	1 year
Successful applications forms and CVs	For duration of employment + 5 years
References received	For duration of employment + 5 years
Statutory sick records, pay, calculations, certificates etc.	For duration of employment + 5 years
Annual leave and holiday pay records, including entitlement, leave taken and carried forward, pay calculations and payments in lieu on termination	At least 6 years from the date each record was made under regulation 16B Working Time Regulations 1998, inserted by the Employment Rights Act 2025 with effect from 6 April 2026. Retain longer only for a documented lawful need or hold.
Unpaid leave/special leave	For duration of employment + 5 years
Annual appraisal/assessment records	Current year and previous 2 years
Time Control Records	6 years
Disclosure and Barring Service (DBS) certificate information	Only as long as necessary after the relevant decision, normally no longer than 6 months; see 9.4 for exceptions, secure disposal and the limited check record.
Personnel files and training records	5 years after employment ceases
Disciplinary or grievance investigations - proved -Verbal –Written –Final warning - Anything involving children	 Warning remains active for the period stated in the disciplinary decision; retain only necessary case evidence under the rule below. Warning remains active for the period stated in the disciplinary decision; retain only necessary case evidence under the rule below. Warning remains active for the period stated in the disciplinary decision; retain only necessary case evidence under the rule below.

	Safeguarding records: retain under a separately documented, case-specific safeguarding rule and any inquiry or legal hold, with specialist advice. Involvement of a child alone does not justify keeping all information permanently.
Disciplinary or grievance investigations - unproven	After investigation and appeal close, review promptly and remove unnecessary material. Board policy: retain a proportionate outcome and necessary case evidence for up to 6 years from closure where justified for legal claims or accountability, with restricted access; preservation holds override routine disposal.
Statutory Maternity/Paternity records, calculations, certificates etc	At least 3 years after the end of the tax year in which the statutory pay was paid; retain payroll evidence under the applicable 7-year finance rule, limiting supporting sensitive information to what is necessary.
Wages/salary records, overtime, bonuses, expenses etc	7 years
Right-to-work check evidence and date of check	For the duration of employment and 2 years after employment ends, then securely dispose unless a specific legal hold applies.

For proved disciplinary and grievance cases, Board policy is to retain necessary case evidence for up to 6 years from final closure where justified for legal claims or accountability, with restricted access and earlier removal of unnecessary material. Expired warnings must not be treated as live warnings. Safeguarding rules and preservation holds take precedence.

Corporate

Minutes and reports of Committee meetings	Indefinitely
Minutes and reports for Special Committee meetings	Indefinitely
Minutes and reports of sub-committees	Indefinitely
Notes and reports of working groups	Indefinitely
Policies and procedures	Retain current versions; preserve superseded approved versions and their approval history as corporate archival records. Remove unnecessary working drafts after approval, subject to holds.
Asset Management records	Indefinitely
Asset management reports	Indefinitely
Internal audit records	7 years
Internal audit fraud investigation	7 years from date of final outcome of investigation
Risk register	Indefinitely
Risk management reports	Indefinitely
Performance reports	Indefinitely

Equalities data	Retain genuinely anonymised statistical outputs as needed. Review identifiable equality-monitoring data annually; erase or anonymise once the documented monitoring purpose ends, unless a justified legal hold applies.
Questionnaire data	Retain identifiable responses only for the documented survey purpose, with a review on completion; erase or anonymise when no longer necessary. Anonymised statistical outputs may be retained.
Details regarding burials	Indefinitely
Drivers log books and mileage	Duration of ownership
Vehicle maintenance and registration records (all necessary certificates, MOT certificates, test records and vehicle registration documents etc)	2 years after vehicle disposed of
Fuel usage records	7 years
Deeds of land and property	Indefinitely
Land and property rental agreements	6 years after expiry of the agreement
Property evaluation lists	Indefinitely
Lease agreements, variation and valuation queries	6 years after the expiry of the agreement
Documentation referring to externally funded projects	7 years
Booking diaries	3 years
Electronic booking information (where applicable)	Board policy: 3 years after the booking, unless a documented financial rule or hold requires longer. Anonymise statistics; do not retain identifiable bookings indefinitely for statistics.
Premises License applications	Indefinitely
Constitution, drainage-district boundaries, confirmed byelaws and statutory orders; approved Board minutes and Annual Governance and Accountability Returns	Permanent corporate archive; minimise incidental personal data and retain a controlled authoritative version.
Drainage rate books, valuation lists, rate-setting and special-levy resolutions	Board policy: preserve final approved books, lists and resolutions permanently as statutory and historical corporate records; routine billing, collection and recovery records for 7 years after the relevant financial year or final settlement, whichever is later, subject to holds.
Land drainage and byelaw consents: decisions, approved plans, conditions and material variations	Board policy: retain the authoritative consent and plans for the life of the consented structure or activity and review on removal or cessation for permanent archival value or continuing rights and liabilities. Remove unnecessary personal and duplicate working material.

Drainage assets, watercourse maps, engineering designs, easements, access rights and capital works records	Board policy: retain authoritative rights, designs and asset history for the life of the asset or right; on cessation review for permanent preservation, residual liability and the applicable contract or deed period before disposal.
Routine watercourse and asset inspection, maintenance and operational work records	Board policy: 7 years after completion or closure; preserve significant asset-history and flood-risk evidence with the asset record. Longer safety, contract, grant or legal-hold rules take precedence.
Flood incidents, environmental assessments, biodiversity and water-level management records	Board policy: 7 years after closure or supersession, then appraise for permanent public-interest or operational preservation. Retain significant flood events, baseline evidence and material decisions where justified; minimise personal details.
Consent refusals, withdrawn applications, complaints and civil enforcement case files	Board policy: 6 years after final closure or appeal, subject to legal advice and holds. Retain authoritative decisions affecting enduring rights with the relevant consent or land record. Before processing criminal-enforcement data, confirm the applicable Data Protection Act 2018 regime and safeguards; do not assume UK GDPR alone governs law-enforcement processing.

Health & Safety

Health and Safety Accident books	At least 3 years after the last entry. Preserve relevant accident and exposure records for longer where occupational disease, asbestos/COSHH health-record duties, a claim or a preservation hold requires it; do not apply the ordinary accident-book period to statutory health-surveillance records.
Statutory health-surveillance records for employees exposed to asbestos or hazardous substances under the Control of Asbestos Regulations 2012 or Control of Substances Hazardous to Health Regulations 2002 (COSHH)	At least 40 years from the last entry where required by the applicable regulations. Keep employer health records separate from confidential clinical records held by the occupational health professional.
Medical examination certificates under the Control of Asbestos Regulations 2012	At least 4 years from issue under regulation 22(4); this does not replace the separate 40-year health-record requirement.
Records relating to accidents person over 18 years	3 years from date of accident
Records relating to accidents person under 18 years	Until 21st birthday

Asbestos records for premises/property including survey and removal records	40 years
All inspection certificates (Gas Safe, FENSA etc)	Board policy: at least 2 years and until superseded where the certificate remains needed to demonstrate safety or compliance. Apply the specific statutory rule for the equipment or premises; do not destroy an operative certificate merely because 2 years have elapsed.
Repairs job sheets	2 years
Periodic machinery inspection tests (PAT, equipment calibration etc)	Board policy: at least 2 years and at least until the next required inspection is recorded. Apply any longer equipment-specific rule, including LOLER; see plant and equipment testing below.
Warranties	10 years
Documents relating to the process of collecting, transporting and disposal of general waste	3 years
Documents relating to the process of collecting, transporting and disposal of hazardous waste	10 years
Plant and equipment testing	PUWER inspection results: at least until the next inspection is recorded. For LOLER records, apply regulation 11: periodic thorough-examination reports until the next report or 2 years, whichever is longer; lifting-accessory reports 2 years; initial equipment and installation records for the applicable life or period of use. Retain longer for a documented safety need or hold.
Risk Assessment Forms	Keep current assessments while the activity or risk remains; Board policy: retain superseded versions for 3 years after replacement or activity ends, and longer where needed for exposure history, claims or a preservation hold.
Manual Handling Assessment Forms	Keep current assessments while applicable; Board policy: 3 years after replacement or activity ends, subject to longer exposure, claim or preservation requirements.

Additional Items

Approved Minutes	Indefinite
Draft/Rough notes taken at meeting	Until minutes are approved, then securely dispose of unnecessary drafts and rough notes, unless they contain unique evidence required for a request,

	claim, investigation or other preservation hold.
CCTV	Board default: 14 days, only where justified for the stated purpose and implemented in the system. Preserve relevant incident or requested footage under a documented hold with review dates. Apply the approved CCTV policy and record any system-specific period; storage capacity alone must not determine retention.
Meeting Recordings	Board default: delete when minutes are approved or after 100 days from recording, whichever is earlier, unless a documented lawful need requires longer. The Clerk must record and review any extension, including a Chair's request. Preserve relevant extracts under a hold; server defaults must not cause premature loss or unnecessary retention.

June 2023 Amendments

- Removed reference to "Unusual Incident Report"

June 2025 Amendments

- Added reference to Meeting Recordings in Additional Items

November 2026 Amendments

- Updated the legal framework to the UK GDPR and Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, including the new data protection complaints requirements.
- Clarified retention start events, statutory minimums, justified Board policy periods and restrictions on indefinite personal-data retention, including equality, questionnaire and booking records.
- Added digital-record security, secure electronic disposal, backup controls, documented disposal authorisation and preservation holds for requests, investigations, claims and inquiries.
- Revised confidential-waste rules so that public availability or potential disclosure does not remove the need for secure disposal.

- Updated DBS handling and criminal-offence-data safeguards; revised disciplinary and safeguarding retention to remove immediate or blanket permanent disposal rules.
- Updated annual-leave and holiday-pay retention for the six-year record-keeping duty effective from 6 April 2026; added right-to-work evidence and clarified pension and tax-record treatment.
- Revised sealed-contract and insurance retention and updated health-surveillance, asbestos and equipment-inspection provisions to protect statutory and liability evidence.
- Added drainage-board records covering rates and levies, byelaws, consents, watercourses, assets, operational works, flood incidents, environmental evidence and enforcement.
- Replaced discretionary or server-led recording retention with documented necessity, deletion and preservation controls for CCTV, meeting recordings and draft meeting notes.