Upper Medway Internal Drainage Board

Subject Access Request Policy

1. Scope

Routine requests for personal data may be handled through the Board's normal business processes where these provide the information requested and meet the applicable data protection requirements. A request is not excluded from the right of access merely because it is routine or informal. Any request that cannot be fully satisfied through normal business processes must be referred promptly to the Data Protection Officer.
This policy applies to personal data processed by Upper Medway Internal Drainage Board (the Board), or held on its behalf, under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025. It includes electronic and paper records relating to identifiable living individuals, including ratepayers, landowners, staff, Board members and complainants. Public-authority rules for unstructured manual personal data must also be considered; paper records must not be excluded merely because they are unstructured.
Requests for a person's own personal data are handled as SARs, not under the Freedom of Information Act 2000 (FOIA) or Environmental Information Regulations 2004 (EIR). Requests for other recorded information, including drainage and environmental information, must be assessed separately under FOIA or EIR, as appropriate. Mixed requests must be handled under each applicable regime and its own deadlines. The Data Protection Officer must obtain specialist advice where processing may fall under the separate law-enforcement regime in Part 3 of the Data Protection Act 2018.

Data subjects are entitled to ask:

- Confirmation whether the Board processes their personal data and, where it does, access to that data and the following supplementary information:
    - the purposes of processing and categories of personal data;
    - the specific recipients to whom the data has been or will be disclosed, including overseas recipients; where identifying them is impossible or manifestly unfounded or excessive, the categories of recipients instead;
    - the retention period, or the criteria used to determine it; rights to request rectification, erasure or restriction and to object to processing; and rights to complain to the Board and the Information Commissioner's Office (ICO).
- A copy of their personal data and any available information about its source where it was not collected from them, together with the appropriate safeguards for transfers to a third country or international organisation, where applicable.
    - Whether automated decision-making, including profiling, is used and, where applicable, meaningful information about the logic involved and its significance and envisaged consequences for them.

2. Responsibilities

The Board remains accountable as controller for compliance with this policy. The Data Protection Officer coordinates SAR handling, advises on compliance, monitors the procedure and reports on requests and concerns.

All staff and Board members must recognise and promptly refer requests to the Data Protection Officer, preserving the original date of receipt. Relevant record holders and processors must assist promptly with searches and secure disclosure. The Clerk must ensure cover during absence, adequate resources and

accessible, published contact routes for requests and complaints. The Data Protection Officer must review this policy annually and when legislation or ICO guidance changes.

3. Procedure

3.1 A SAR may be made verbally or in writing, including by email or social media, to any part of the Board. No prescribed form, reference to legislation or "official" application is required. Record the request and date received and refer it promptly to the Data Protection Officer. A representative may act with appropriate authority, which must be checked before disclosure.

3.2 Verify identity proportionately. Additional evidence may be requested promptly only where there are reasonable doubts about identity, and only to the extent necessary. Do not routinely require a passport, driving licence or other photographic identification where identity is already known or can be verified by less intrusive means. Protect any evidence supplied and retain it only as long as necessary.

3.3 Individuals may request all their personal data without identifying particular records or where they are held. Seek clarification promptly only where it is reasonably required to identify the information or processing activities requested; explain why it is needed and assist the requester. Do not require the person to narrow a valid request. Where a lawful clarification pause applies, record its start and end and the revised deadline; the response period pauses from the clarification request and resumes on the day after clarification is received. A question about response format does not pause the clock.

3.4 Respond without undue delay and within one calendar month of receipt, not a fixed 28 days. Where identity or representative-authority evidence is reasonably required, or a lawful fee is requested, calculate the period from receipt of that information or fee. Record receipt, any necessary evidence, lawful clarification pauses and the deadline. The deadline is the corresponding date in the following month, or the last day if there is no corresponding date; if it falls on a weekend or public holiday, use the next working day. Where necessary because of complexity or the number of requests from the same person, extend by up to two further months and notify the requester of the extension and reasons within the initial one-month period.

3.5 The Data Protection Officer coordinates collection and review of the requested personal data in time for the response deadline. The right is to personal data, not automatically to every complete document mentioning the individual; supply enough context to make the information intelligible.

Collection must involve reasonable and proportionate searches, including:

3.1..1.1 Locating the requested personal data using the Board's data map and relevant record holders and processors; and

- Searching relevant electronic systems, email and business messaging, paper files, archives and backup records where appropriate. Consider personal data in rating and landowner records, drainage and consent correspondence, complaints, employment records, minutes and CCTV where held. Include Board business records held by staff, members or service providers, including on personal devices or accounts where relevant. Record the locations, search terms

and scope, and justify any search considered unreasonable or disproportionate; continue searching other relevant sources.

3.6 Maintain a secure SAR register recording receipt, scope, identity and authority checks, deadlines, clarification pauses, extensions, searches, exemption and redaction decisions, correspondence, and the response and delivery date. Preserve information needed to answer the request: it must not be altered, concealed, erased or destroyed with the intention of preventing disclosure. Restrict access to SAR records and retain them only for the justified period in the Board's retention arrangements.

3.7 Review information about other identifiable individuals case by case. Disclose mixed personal data where the other person consents or it is reasonable to disclose without consent, considering confidentiality, the nature of the information and all relevant circumstances. Consent is not an absolute requirement. Where withholding is justified, redact only what is necessary and provide the requester's remaining personal data. Record the balancing decision and check redactions are effective and irreversible.

3.8 Apply exemptions only where the relevant statutory conditions are met, on a case-by-case basis and only to the extent justified. Record the legal provision, reasons and any required prejudice or other statutory test; do not treat the following as automatic exclusions. Potentially relevant exemptions include:

3.1..1.1 Crime prevention or detection, or taxation, where disclosure would be likely to prejudice the relevant purpose.

3.1..1.2 Records of intentions in negotiations with the requester, where disclosure would be likely to prejudice those negotiations.

3.1..1.3 Management forecasting or planning, where disclosure would be likely to prejudice the conduct of the business or activity.

- Confidential references that meet the statutory exemption; do not limit consideration to references issued by the Board.

3.1..1.1 Scientific or historical research, statistics or archiving in the public interest, only where the applicable statutory conditions and safeguards are met.

3.1..1.2 Information covered by legal professional privilege. Seek specialist advice where the applicability of any exemption is uncertain and disclose non-exempt information.

SARs are normally free of charge. The Data Protection Officer may authorise a reasonable administrative-cost fee or refusal only where a request is demonstrably manifestly unfounded or excessive, and a reasonable fee for further copies where permitted by law. Document and justify the decision; a request for all data or a large volume is not, by itself, excessive. If refusing to act, explain the reasons without undue delay and within one month, subject to lawful restrictions on the explanation, and inform the person of their right to complain to the Board and the ICO and to seek a judicial remedy. Explain any partial withholding on the same basis.

3.9 Provide confirmation whether personal data is processed, a copy where held and the supplementary information set out in Scope. Use clear, plain language, explain codes, and provide an accessible format with reasonable adjustments where needed. Record the information disclosed and delivery

date in a schedule. Check the recipient and delivery method, use appropriate security, and verify that redactions, hidden text and metadata do not disclose withheld information.

3.10 Where the request is made electronically, provide the information in a commonly used electronic format unless the person requests otherwise. Consider accessibility and reasonable adjustments rather than insisting on one format.

3.1..1.3 PDF may be used where suitable and accessible; provide another appropriate format or a paper copy where required.

11. Individuals may complain about SAR handling to the Board through the Clerk or Data Protection Officer, verbally or in writing, including electronically. Publish an accessible complaints route and pass complaints received through other Board channels promptly to the responsible officer. Acknowledge complaints within 30 days of receipt, investigate appropriately without undue delay, keep the person informed, and communicate the outcome and any corrective action without undue delay. Record the complaint and outcome securely and explain the right to complain to the ICO and seek a judicial remedy.

November 2022 Alterations

- Removed reference to LMIDB
- Minor formatting

November 2025 Alterations

- Added example of ID required
- Removed reference to a SAR application form, replaced with official SAR application
- Changed ‘one month’ to 28 days for definition

November 2026 Alterations

- Removed the routine-request exclusion and clarified the UK GDPR/DPA 2018 scope, including data held on the Board’s behalf, public-authority paper records and the distinction between SARs and FOIA/EIR requests.
- Removed the requirement for an official application or identification of data locations, and replaced mandatory photographic ID with proportionate identity and representative-authority checks.
- Corrected the response period to one calendar month and clarified lawful extensions, clarification pauses and deadline recording under the Data (Use and Access) Act 2025.
- Introduced documented reasonable and proportionate searches, with Board-specific record sources, processor assistance and preservation of requested information.
- Corrected the third-party disclosure test and conditional application of exemptions; clarified lawful fees, refusals and complaint and court rights.
- Expanded the information supplied with SAR responses and required secure, accessible disclosure rather than a mandatory PDF-only response.
- Added statutory data protection complaints handling, including acknowledgement within 30 days and investigation, updates and outcomes without undue delay.