Upper Medway Internal Drainage Board
Breach Notification Policy

1. Scope

1.1 This policy applies to personal data breaches under Articles 33 and 34 of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended, including by the Data (Use and Access) Act 2025. It covers all personal data processed by Upper Medway Internal Drainage Board (the Board), in electronic or paper form and whether held by the Board or on its behalf.

1.2 The Board is the controller where it determines the purposes and means of processing personal data; the Clerk or Data Protection Lead acts on its behalf and is not personally the controller. A processor processes personal data on a controller's instructions. The Board must identify and document its role for each processing activity, including any joint-controller arrangements. The Board may be a controller for some activities and a processor for others.

1.3 A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes loss of confidentiality, integrity or availability, such as a misdirected email, lost paper file, unauthorised access or loss of access to personal data.

2. Responsibility

2.1 All employees, temporary staff, contractors, third-party users and Board members (elected and appointed, including councillor members) must follow this policy. Actual or suspected personal data breaches must be reported immediately to the Clerk or designated Data Protection Lead, without waiting for proof or completion of an investigation.

2.2 The Board retains accountability for compliance. The Clerk or designated Data Protection Lead coordinates the response and notifications, with timely involvement of the Board's Data Protection Officer (DPO). As a public authority, the Board must appoint a DPO in accordance with Articles 37–39 UK GDPR, with independence, appropriate resources and direct access to the Board. The Data Protection Lead is not automatically the statutory DPO; any combined role must avoid conflicts of interest.

2.3 The Clerk must maintain and circulate current incident-reporting contacts, including a nominated deputy and out-of-hours escalation arrangements. If the Clerk or Data Protection Lead cannot be reached, the reporter must escalate immediately to the nominated deputy or Chair. The response lead must take prompt, proportionate containment and recovery action, preserve evidence and involve relevant IT support or processors. Urgent notifications must not await a Board meeting or prior Board approval.

2.4 The response lead must maintain a restricted-access Internal Breach Register for all personal data breaches, whether or not reported externally, recording the facts, discovery and awareness times, effects, risk assessment, decisions and reasons, remedial action and notifications. Suspected incidents must also be logged and their outcome recorded. After each breach, review causes and controls, assign corrective actions and report proportionately to the Board without unnecessary personal data. Review this policy and test contact and escalation arrangements at least annually.

3. Procedure – Breach Notification Data processor to Data Controller

3.1 Where the Board acts as a processor, the Clerk or designated Data Protection Lead shall notify the relevant external controller without undue delay after the Board becomes aware of a personal data breach, using the agreed contractual reporting route. This duty applies to all such breaches and is not conditional on the

Board's risk assessment. Processors acting for the Board must be contractually required to notify the Board without undue delay and assist with investigation and compliance.

3.2 The Data Protection Lead shall record the breach and the controller notification in the Internal Breach Register and promptly provide the available facts, affected data and individuals, likely effects and containment measures.

3.3 Notify the controller's agreed incident contact by telephone or secure email, using an alternative agreed route if the normal system is unavailable or compromised. Record the time and recipient and send secure written confirmation; do not delay the initial notification while collecting further details.

3.4 Seek and record acknowledgement of receipt. If it is not received promptly, follow up by telephone and escalate to the controller's alternative contact. Provide further information without undue delay as it becomes available.

4. Procedure – Breach Notification Data Controller to Supervisory Authority

4.1 Where the Board acts as controller, the Clerk or designated Data Protection Lead shall arrange notification to the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours after the Board becomes aware of a personal data breach, unless the breach is unlikely to result in a risk to individuals' rights and freedoms.

4.2 The Data Protection Lead, with DPO advice, shall assess and document the likelihood and severity of harm to individuals, considering the nature and sensitivity of the data, identifiability, numbers affected, vulnerable individuals, likely consequences and the effectiveness of protection and containment. Record reasons for notifying or not notifying the ICO or individuals, and reassess as facts emerge. Uncertainty must not delay a required notification.

4.3 Record when the Board has a reasonable degree of certainty that a security incident has compromised personal data: this is the awareness point for the 72-hour period, which includes weekends and bank holidays. Do not wait for a full investigation. If notification is made after 72 hours, give the ICO reasons for the delay. Where details are incomplete, submit the available information within the required period and supply further information without undue further delay.

4.4 The Clerk or designated Data Protection Lead shall notify the ICO on behalf of the Board, providing at least the information in clauses 4.5–4.11, so far as available:

4.5 A description of the nature of the breach.

4.6 The categories of personal data records affected.

4.7 The categories and approximate number of data subjects affected, where possible.

4.8 Approximate number of personal data records affected.

4.9 The name and contact details of the DPO or other contact point where further information can be obtained.

4.10 Likely consequences of the breach.

4.11 Any measures that have been or will be taken to address the breach, including mitigation.

4.12 Where all required information cannot be supplied at once, provide it in phases without undue further delay, identifying outstanding information and retaining a record of each submission.

4.13 Use the ICO's current personal data breach reporting service; a pre-existing personal contact at the ICO is not required. Record the submission, date and time, reference number and subsequent correspondence in the Internal Breach Register.

4.14 Submit notification through the ICO's current online reporting route or contact the ICO for an alternative if that route is unavailable. Technical difficulties must be escalated promptly; retain evidence of attempted reporting.

4.15 Retain the ICO acknowledgement and follow up promptly if it is not received. Respond to requests for further information and record all subsequent updates and action.

5. **Procedure – Breach Notification Data Controller to Data Subject**

5.1 Where a personal data breach is likely to result in a high risk to individuals' rights and freedoms, the Board shall communicate directly with affected individuals without undue delay, subject only to the exceptions in clauses 5.3–5.5. The Clerk or Data Protection Lead shall coordinate this with DPO advice, recording the decision and reasons.

5.2 The communication must describe the nature of the breach in clear and plain language, give the name and contact details of the DPO or other contact point, explain the likely consequences and measures taken or proposed to address the breach and mitigate harm. Include practical advice on how individuals can protect themselves. This communication must not wait for the ICO investigation or the full internal investigation to finish.

5.3 Individual communication is not required where appropriate technical and organisational protection measures were applied to the affected personal data and render it unintelligible to unauthorised persons, such as effective encryption. Assess whether the protection remains effective, including whether encryption keys were compromised, and record the evidence supporting reliance on this exception.

5.4 Individual communication is not required where subsequent measures ensure that the high risk to individuals' rights and freedoms is no longer likely to materialise. Record the measures and evidence supporting this conclusion; this exception does not remove the separate duty to notify the ICO where applicable.

5.5 If individual communication would involve disproportionate effort, the Board must instead make a public communication or take a similar measure which informs affected individuals in an equally effective manner. Record the justification and chosen method, avoid unnecessary disclosure of personal data, and reassess whether affected individuals can be reached directly.

5.6 The ICO may require the Board to communicate the breach to affected individuals, having considered the likelihood of high risk, or may decide that an Article 34(3) exception applies. The Board shall comply with any such requirement and record the communication and subsequent action.

- Changed references of CEO to Clerk

November 2026 Alterations

- Updated the legal framework to UK GDPR and the Data Protection Act 2018 as amended, including the Data (Use and Access) Act 2025, and defined personal data breaches across paper and electronic records.
- Clarified the Board's controller and processor responsibilities, coverage of all Board members, statutory DPO arrangements and immediate internal escalation, including deputy and out-of-hours cover.
- Corrected the ICO reporting threshold and the 72-hour period from awareness; strengthened risk assessment, phased reporting and the required notification information.
- Corrected notification to affected individuals, including the high-risk threshold, required communication content and the limited Article 34 exceptions.
- Required records of all breaches and notification decisions, prompt containment, evidence preservation and corrective action; replaced unspecified reporting methods with operational notification and follow-up procedures.