Upper Medway Internal Drainage Board
Information Technology (IT) and Artificial Intelligence (AI) Use Policy

The UMIDB recognises the critical importance of secure, responsible, and ethical use of Information Technology (IT), including Artificial Intelligence (AI), to support its operations. This policy sets out the principles for IT usage across the organisation and outlines expectations around data protection, security, and transparency, particularly in the context of emerging AI tools and capabilities.

Purpose and Scope

This policy applies to:

- All UMIDB staff, Board members, contractors, and temporary personnel.
- All devices, networks, platforms, software, cloud systems, and AI tools used in connection with UMIDB operations.

Legal and Regulatory Framework

This policy must be applied in accordance with the following legislation, as amended and in force:

- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 – govern the lawful processing, security and protection of personal data and individuals' rights.
- Freedom of Information Act 2000 (FOIA) – sets access expectations for recorded information held by UMIDB.
- Environmental Information Regulations 2004 (EIR) – regulates access to environmental data.
- Computer Misuse Act 1990 – outlines criminal offences involving unauthorised access to computer systems.
- Land Drainage Act 1991 and Flood and Water Management Act 2010 – provide the statutory context for the Board's drainage and flood-risk management functions; IT and AI do not alter statutory powers or delegated decision-making authority.
- Equality Act 2010, including the public sector equality duty – requires due regard to eliminating unlawful discrimination, advancing equality of opportunity and fostering good relations when exercising public functions.

Policy Commitments

The UMIDB will:

- Ensure all IT systems and data are used in line with security, privacy, and legal obligations.
- Maintain up-to-date antivirus, firewall, and threat detection systems on all networks and devices.
- Provide staff and contractors with training and guidance on secure and ethical IT use, including role-specific training on the safe use of AI tools. AI training must cover information handling, security, checking the accuracy of outputs, and when and how to seek advice. Training must be recorded through the Board's usual training records.
- Use AI technologies only where they are clearly justified, transparent, and lawful.
- Ensure AI use is subject to appropriate human oversight and complies with data protection, fairness and accountability principles.

- Maintain logs of AI-assisted decisions, where appropriate, to ensure traceability and governance.

Use of Artificial Intelligence (AI)

AI refers to systems that perform tasks requiring human intelligence such as analysis, prediction, language processing, or automation. UMIDB acknowledges both the benefits and risks of AI.

The Clerk will maintain a register of approved AI tools and platforms, setting out their permitted uses and the information each may receive. The register must be available to all users and maintained separately from this policy, with each entry identifying the approved tool and account type, data restrictions, responsible officer, and approval and review dates. Approval covers only the recorded use, account and data restrictions, including AI features embedded in other software. Users must obtain the Clerk's written approval before using other tools or submitting information outside those restrictions; the Data Protection Officer (DPO) must be consulted where personal data is involved.

Before approval, the responsible officer must document the purpose, expected benefits, risks and controls for the proposed use, proportionate to its impact. Assess accuracy, bias, equality impacts, confidentiality, security and effects on ratepayers, landowners and the public. Record how due regard has been given to the public sector equality duty before decisions are taken. Material changes to the tool, supplier terms, data or purpose require reassessment.

AI tools may be used to:

- Improve internal efficiency (e.g. document summarisation, scheduling, or drafting).
- Support public communications or internal policy development.
- Assist with data analysis, modelling, or asset management in line with Board functions.

AI tools must not be used for:

- Processing personal data without a valid legal basis under UK GDPR.
- Making solely automated decisions with legal or similarly significant effects on individuals, including decisions on drainage rates, consents or enforcement. This is a Board policy restriction, not a statement that all such decisions are prohibited by UK law. AI-assisted decisions must receive meaningful review by an authorised person who can question and change the outcome; statutory delegations and appeal rights must be preserved.
- Replacing critical human judgement in matters of safety, policy, or legality.
- Circumventing access controls or confidentiality policies.

AI outputs must be checked by a suitably competent person before they are relied upon or shared. Checks must be proportionate to the task and cover accuracy, sources, legal requirements, and calculations where relevant. The user remains responsible for ensuring these checks are completed.

AI use must fall within a recorded approval by the Clerk. New or materially changed uses require approval before deployment, with DPO advice where personal data is involved and Board approval where required by the Board's scheme of delegation. DPO advice does not replace the Board's accountability or authorise otherwise unlawful processing.

AI must not directly control pumps, sluices or other operational equipment, or change telemetry or control-system settings, unless a separate Board-approved safety and cyber-security assessment, testing, authorised change control and effective human override are in place. Hydraulic modelling, flood-risk advice and

engineering outputs must be validated by a suitably qualified person against reliable data, local conditions and model limitations before operational reliance.

GDPR and Data Handling Expectations

- All users must safeguard the confidentiality, integrity, and availability of personal data.
- Personal data must only be accessed where necessary for legitimate work tasks.
- Assess proposed personal-data processing before it begins and document whether a Data Protection Impact Assessment (DPIA) is required. Complete a DPIA before processing likely to result in high risk to individuals' rights and freedoms, seek DPO advice, and review it when risks change. Where residual high risk cannot be reduced, consult the ICO before processing begins.
- Personal data and other confidential Board information must not be entered into AI tools unless the particular tool, account, purpose and information are explicitly approved. Use only the minimum necessary information and anonymise it where practicable; removing names alone may not prevent identification. Supplier reuse of Board information for model training is prohibited unless separately assessed and expressly authorised on a lawful basis.
- Report any suspected personal data breach immediately to the Clerk or DPO, following the Board's Breach Notification Policy. The Board must document all personal data breaches and reporting decisions, notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to result in a risk to individuals' rights and freedoms, and inform affected individuals without undue delay where high risk requires it, subject to applicable statutory exceptions.

Before processing personal data, document the purpose and applicable Article 6 lawful basis; for statutory functions identify the relevant legal obligation or public task and its basis in law. Neither legitimate interests nor recognised legitimate interests is available to a public authority when performing its public tasks. Special category and criminal offence data require the additional conditions and safeguards applicable under Articles 9 and 10 and the Data Protection Act 2018. Update privacy information and processing records to explain relevant AI use and enable individuals to exercise their rights.

Before appointing an IT or AI supplier, assess its security, data use, retention, subcontractors and access arrangements, and document the controller/processor roles. Where a supplier processes personal data on the Board's behalf, put an Article 28-compliant contract in place, including confidentiality, security, assistance with rights and breaches, audit and return or deletion of data. Identify restricted international transfers, including overseas access, and ensure a lawful transfer mechanism and any required data protection test or transfer risk assessment are in place before transfer.

The Board must provide an accessible route for data protection complaints, including complaints about AI use. Users must forward these promptly to the Clerk or DPO. The Board must acknowledge complaints within 30 days of receipt, investigate and keep complainants informed without undue delay, and communicate the outcome without undue delay. Privacy information must explain how to complain and the right to complain to the ICO. Requests to exercise data protection rights must be handled separately within the applicable statutory timescales.

Acceptable Use Requirements

Users must:

- Use UMIDB IT systems and AI tools only for authorised business purposes.

- Refrain from using personal devices or unapproved software to access Board systems or sensitive data.
- Report suspected phishing, malware, or cyberattacks without delay.
- Protect login credentials and never share passwords or access rights.
- Comply with any restrictions around cloud storage, remote working, and mobile device usage.

The Clerk must ensure risk-based security arrangements cover supported software and timely security updates, least-privilege access, multi-factor authentication where available, appropriate encryption, prompt removal of leavers' access and periodic access reviews. Maintain protected backups and test restoration and incident-recovery arrangements. Maintain an inventory of operational technology where used, including telemetry and pump or sluice controls; restrict and monitor supplier remote access, separate it appropriately from office systems, and maintain tested safe isolation and continuity arrangements. These are Board security controls informed by NCSC guidance, not a claim that each measure is universally prescribed by statute.

Keep Board business records in approved corporate systems, including material AI prompts, outputs, source material, human checks and reasons supporting decisions where needed for accountability. Apply the Board's retention and disposal rules; suspend deletion where records are required for information requests, complaints, investigations or litigation. Recorded information held by or on behalf of the Board may fall within FOIA or EIR, including environmental modelling and drainage information. Refer requests promptly to the Clerk; confidentiality or use of AI does not itself exempt records from disclosure. Respect copyright, database rights and licence restrictions when uploading material or using outputs.

Governance and Accountability

The Board retains overall accountability for this policy and for personal-data processing where it acts as controller. The Clerk is responsible for implementation and operational approvals within delegated authority. Day-to-day IT security work may be delegated to appropriate officers or external service providers (GrayIT), but accountability remains with the Board. The Board must appoint an independent, appropriately qualified and resourced DPO, publish their contact details and notify the ICO. The DPO advises and monitors compliance, reports to the highest management level and must not be assigned conflicting operational decision-making responsibilities.

Staff and Board members are expected to uphold this policy in all operational activities. Failure to comply may result in disciplinary action or termination of access rights.

Monitoring and Review

- UMIDB will undertake necessary and proportionate logging and review of IT usage and AI implementation for defined security and compliance purposes. Document the lawful basis, inform users of the nature, extent and purposes of monitoring, restrict access to logs and set justified retention periods. Complete a DPIA before monitoring likely to result in high risk. This policy does not authorise unrestricted or routine covert monitoring.
- This policy will be reviewed annually, or sooner following legislative changes, significant incidents, new risks or relevant regulatory guidance, including from the Information Commission (ICO). The Clerk must report material compliance risks and significant incidents to the Board and arrange approval of substantive policy changes.
- AI use cases will be periodically reviewed to ensure they remain ethical, lawful, and aligned with public expectations.

Amendments

November 2026

- Added a requirement for the Clerk to maintain a register specifying approved tools, permitted uses, and the information each may receive.
- Added mandatory checks by a suitably competent person before AI outputs are relied upon or shared.
- Expanded the training commitment to include role-specific AI training.
- Updated the legal framework for the Data (Use and Access) Act 2025 and the Board's statutory drainage functions, and added explicit equality-duty safeguards for AI use.
- Clarified Board accountability, independent DPO oversight and approval of new or changed AI uses; retained the Board's restriction on significant solely automated decisions and protected statutory decision-making and appeal rights.
- Strengthened lawful-basis, DPIA, supplier-contract and international-transfer safeguards, and restricted confidential information and supplier model-training use.
- Added statutory breach-notification requirements and the data protection complaints procedure, including acknowledgement within 30 days.
- Added risk-based cyber-security, backup and recovery controls and safeguards for operational technology, engineering outputs and AI control of equipment.
- Added AI decision-record and FOIA/EIR preservation requirements, proportionate monitoring safeguards and annual policy review with reporting of material risks to the Board.