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 aligns with the following legal requirements:

- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 – governs the processing, storage, and protection of personal data.
- 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.

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 training and guidance to staff and contractors on secure and ethical IT usage.
- Use AI technologies only where they are clearly justified, transparent, and lawful.
- Ensure AI use is subject to appropriate human oversight and comply with data protection, fairness, and countability 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.

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 autonomous decisions that significantly affect individuals or public rights.

Replacing critical human judgement in matters of safety, policy, or legality.
Circumventing access controls or confidentiality policies.

Any use of AI must be approved by the Clerk or designated Data Protection Officer, especially where personal data or decision-making is involved.

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.
- AI or IT systems used for processing personal data must be assessed for risk and documented accordingly in a Data Protection Impact Assessment (DPIA), where required.
- Personal data must not be uploaded to AI platforms that store or reuse data unless explicitly permitted and compliant with UK GDPR.
- Any suspected data breach must be reported immediately to the Clerk or designated officer.

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.

Governance and Accountability

The Clerk is responsible for overall policy compliance. Day-to-day oversight of IT security and AI use may be delegated to appropriate officers or external service providers (GrayIT).
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 log and review IT system usage and AI tool implementation to ensure accountability.
- This policy will be reviewed every two years, or sooner if prompted by legislative changes, new risks, or guidance from regulatory bodies such as the ICO or the Centre for Data Ethics and Innovation (CDEI).
- AI use cases will be periodically reviewed to ensure they remain ethical, lawful, and aligned with public expectations.

Approval

Approved by UMIDB on 11th November 2025