Upper Medway Internal Drainage Board
Cybersecurity and Acceptable Use Policy

The Upper Medway Internal Drainage Board (UMIDB) is committed to protecting its digital infrastructure, systems, and the personal data it holds. As a public body, we have a duty to ensure that data is processed securely, responsibly, and in full compliance with the law. We recognise that strong information governance is essential to maintaining stakeholder trust, safeguarding service continuity, and complying with our statutory obligations.

For reference the Board's Data Protection Officer is Richard Newell of GDPR-Info.com who can be contacted via the office or Clerk.

Purpose and Scope

This policy ensures that UMIDB:

- Protects its information assets—whether digital or physical—against loss, corruption, unauthorised access, or misuse.
- Handles personal data lawfully, fairly, and transparently in line with the UK GDPR and Data Protection Act 2018.
- Assigns responsibilities and implements controls to manage data security risks.

This policy applies to:

- All employees, Board members, contractors, consultants, and any other authorised users of UMIDB's data or IT systems.

Legal and Regulatory Framework

UMIDB is committed to fulfilling its obligations under:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Computer Misuse Act 1990
- The Freedom of Information Act 2000 (where applicable)
- Any standards applicable to public-sector IT security (e.g. Cyber Essentials)

Policy Commitments

UMIDB will:

- Maintain secure IT systems through the use of firewalls, antivirus software, encryption, and access controls.
- Limit access to personal and sensitive data based on user roles and legitimate need.
- Conduct regular data protection and cybersecurity training for all staff and members.
- Have a designated Data Protection Officer (DPO) or equivalent responsible for overseeing compliance and advising on data risks.

- Respond promptly and appropriately to any data breaches, near-misses, or cyber threats in accordance with the Information Commissioner's Office (ICO) requirements.
- Maintain up-to-date data protection policies, privacy notices, and information asset registers.
- Ensure that contractors and service providers handling data on UMIDB's behalf meet equivalent security standards.

Roles and Responsibilities

- Clerk: Has overall responsibility for ensuring the integrity and security of UMIDB's information systems.
- Data Protection Officer (or designated lead): Oversees compliance with data protection law, advises on risk, and monitors processing activities.
- All users: Must follow security procedures, report any suspected breaches, and complete mandatory training.

Incident Reporting and Breach Response

Any actual or suspected data breach must be:

- Reported immediately to the DPO or IT lead.
- Investigated without delay, with appropriate remedial action taken.
- Documented in a breach register.
- Notified to the ICO within 72 hours if required by law.

Monitoring and Review

This policy will be reviewed annually, or earlier if required due to changes in legislation, security best practices, or organisational structure. System access, user activity, and security incidents will be monitored continuously to maintain and enhance our digital resilience.

Delivery Procedures

Access Management
Only authorised users may access UMIDB systems. User accounts will be created, modified, and deactivated by the IT administrator (GrayIT). Two-factor authentication will be used where available.

Acceptable Use
Staff must not install unauthorised software or use systems for personal commercial gain. Emails must be professional and used for work purposes only. Personal data must not be downloaded to unencrypted devices.

Training and Awareness
All users will receive periodic training on phishing, password management, data protection, and safe browsing. IT policy compliance is mandatory.

Incident Reporting

Suspicious emails or activities must be reported immediately to the Clerk or a member of the Board. The Clerk will coordinate response actions with IT support and escalate as needed.

Monitoring and Review

The Clerk will review system and security settings periodically.

This policy will be reviewed annually to reflect changing threats and legal obligations.

June 2026 Amendments

- Added name of DPO to document