March Town Council Information Technology (IT) Policy

1. Purpose

This Policy sets out how March Town Council manages its use of information technology, in line with the Transparency Code for Smaller Authorities (2015) and The Practitioners' Guide (2025 edition).
It seeks to ensure that the Council's digital operations are compliant with date protection laws and that they are both secure and transparent.

2. Scope

This Policy applies to councillors, officers and employees and also to any contractors who access the Council's IT systems which includes, inter alia, desktop and laptop computers, smartphones, email and cloud-based systems, personal devices under Bring Your Own Device (BYOD) provisions and the Council's website and digital publication tools (such as WordPress).

3. Governance

The Clerk shall be the Council's designated Data Protection Officer (DPO) and IT Systems Administrator.

The Personnel and Admin Committee shall oversee implementation and compliance.

4. Data Protection and Security

All processing of personal data shall comply with UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Privacy; All data collection, processing and subject right are governed by the Council's Privacy Policy, published on the Council's website.
Users must familiarise themselves with this document.

Access/Storage; Data is stored securely, with access only granted to authorised personnel. Access must be based on necessity.

Retention; Data shall be retained in accordance with the Council's Data Protection and GDPR Policy and will be securely deleted once no longer required.

Security Controls;

- Password protection and multi-factor authentication (where possible)
- Regular updates and anti-malware software
- Back-ups of essential data in secure locations

5. Use of Personal Devices (BYOD)

Councillors and officers may use personal devices for council business **if explicitly authorised** and subject to compliance with this policy.

Requirements; Devices must be protected by strong passwords, encryption (where possible) and up-to-date antivirus software.

Access to council data and systems on a personal device must be controlled, proportionate to need and subject to regular review.

Data Separation; Council data must be kept separate from personal data using dedicated storage files/areas and apps.

6. Use of Personal Email Addresses

The use of personal email accounts is prohibited for council business.
All correspondence shall be conducted through official council email addresses.
Emails from council-owned domains shall not be forwarded to personal email addresses.
Any breaches of this will be investigated by the Clerk and/or the Personnel and Admin Committee and such measures as deemed appropriate shall be taken in accordance with the Council's disciplinary or governance procedure(s).
Council emails must be stored in compliance with GDPR and Freedom of Information (FOI) requirements.

7. IT Infrastructure and Support

- All Council-owned hardware and software shall be recorded in the Council's Asset Register.
- Devices must be regularly updated and checked for compliance with this Policy.
- Users shall be given such training on IT systems, data handling, data protection policies and regulations, cybersecurity and transparency requirements as necessary.

8. Review

This Policy will be reviewed annually, or sooner in the event of legislative changes or in the event of a significant incident/breach.

9. Data Breach Procedure

March Town Council shall respond promptly to any data breaches or alleged data breaches to comply with GDPR requirements.

10. Data Breach – a Definition

A data breach is a serious security incident that results in the accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to, personal data, examples of which include, inter alia;

- Loss of theft of devices
- Unauthorised access to council emails or files
- Malware or ransomware attacks that attack or threaten to attack Council systems/databases
- Sending personal data to the wrong recipient(s)

11. Reporting a Data Breach

Any councillor, officer, employee or contractor who becomes aware of a data breach or suspected data breach must report it immediately to the Clerk (DPO).

The Clerk shall forthwith assess the severity of the breach and all associated risk and determine what action is required to be taken in mitigation (such as changing of password(s) or disabling access).

12. Investigating a Breach

A full investigation shall be conducted within 72 of the discovery of the breach.
The Clerk/DPO will log the following information;

- Data and time of the breach
- Nature of the breach
- Type/volume of data affected
- Cause and extent of said breach
- Actions taken/to be taken consequent to the breach

13. Notification Requirements

If the data breach is like to result in a risk to an individual's rights and freedoms, the Council **must** notify the Information Commissioners Office (ICO) within 72 hours.

If the breach represents a high risk to said affected individual(s), those individual(s) must be informed at the earliest opportunity, stating the nature of the data breach, likely consequences/outcomes, measures taken to limit or mitigate the risk and information about who to contact for further advice or support.

14. Post-Breach Review and Remediations

The Clerk and Personnel and Admin Committee will ensure lessons are learned and policies, procedures and training are updated as necessary to prevent future breaches. They will prioritise security upgrades and repair/improve any technical issues/faults to prevent recurrence.
Logs of breaches should be reviewed on a regular basis to discover trends and to identify systemic issues.

This Policy was adopted by March Town Council on 3 November 2025 and will be reviewed annually or following either legislative change or a significant incident.