WICKHAM MARKET PARISH COUNCIL

Information Technology Policy

(Assertion 10 – Digital and Data Compliance)

Applies To: Councillors, Clerk/Responsible Financial Officer, staff, contractors, volunteers

1. Purpose

This Information Technology Policy ensures that Wickham Market Parish Council complies with Assertion 10 (Digital and Data Compliance) as introduced in the 2025 Practitioners' Guide. This assertion requires all smaller authorities to have a clear Information Technology Policy covering both council-owned and personal devices.

It defines how digital tools, data and communications must be managed to protect personal information, ensure secure governance, and support accessibility and transparency.

2. Scope

This policy applies to all individuals conducting council business using:

- Council-provided Information Technology systems
- Personal devices used for council work (Bring Your Own Device)
- Council-issued email accounts
- Any platform used to store, transmit or access council data

3. Council Email Use

To meet Assertion 10, councillors and staff must use official council email accounts on a council-owned domain for all communications. Personal email accounts must not be used for council business.

Email Requirements

- All council business must be conducted through council-issued email accounts.
- Email forwarding to personal accounts is prohibited.
- Two-factor authentication must be used where available.
- Strong passwords must be used and changed at least annually.
- Access is revoked when an individual leaves the council.

4. Use of Personal Devices (Bring Your Own Device)

Bring Your Own Device usage is permitted but must meet strict security requirements due to risks such as data leakage, unauthorised access and loss or theft. These risks are highlighted in sector guidance and Information Commissioner's Office findings.

Security Requirements

Anyone using a personal device for council work must:

1. Use only their council email account for council work.
2. Keep devices updated with security patches.
3. Enable device security (password, PIN, biometric lock and encryption where possible).
4. Prevent others from accessing council information on their device.
5. Avoid using personal cloud storage for council documents unless authorised.
6. Report lost or stolen devices immediately to the Clerk.

5. Data Protection and General Data Protection Regulation

Assertion 10 emphasises mandatory compliance with United Kingdom General Data Protection Regulation and the Data Protection Act 2018.

Requirements

- The council is the Data Controller.
- The Clerk is the Data Processor.
- Personal data must not be stored unencrypted on any device.
- Approved storage systems must be used.
- Freedom of Information and Subject Access Requests must be followed in line with council procedures.

6. Websites, Accessibility and Published Information

The council must comply with website accessibility standards, including the Web Content Accessibility Guidelines Version 2.2 at Level AA.
In addition, the council must publish required documents in accessible formats under Freedom of Information and transparency regulations.

Requirements

- Maintain an up-to-date accessibility statement.
- Publish accessible versions of documents.
- Regularly check site compliance with Web Content Accessibility Guidelines.

7. Document Handling and Storage

- Documents must be stored only in approved council locations.
- Uncontrolled copies or drafts containing personal information must be deleted securely.
- Removable media may only be used if encrypted and authorised.

8. Cybersecurity and Acceptable Use

Security threats such as phishing or malware require ongoing vigilance as identified in Assertion 10 guidance.

Users Must:

- Complete cybersecurity awareness training when offered.
- Avoid unauthorised apps and software for council work.
- Avoid public Wi-Fi for sensitive tasks unless using a Virtual Private Network.
- Report suspicious emails.

9. Records Management and Retention

- Emails and documents must comply with retention schedules.
- Individuals must not delete council data without permission.
- On leaving the council, individuals must remove all council data from personal devices.

10. Compliance and Enforcement

Compliance with this policy is required to meet Assertion 10 and to complete the Annual Governance and Accountability Return. Non-compliance may trigger audit concerns or regulatory issues.

Breaches may lead to:

- Withdrawal of access
- Investigation under the Code of Conduct
- Reporting to the Information Commissioner's Office if necessary

11. Policy Review

The policy will be reviewed annually or when guidance from the Smaller Authorities' Proper Practices Panel, National Association of Local Councils or Government Digital Service changes.

2. Bring Your Own Device (BYOD) Agreement Form

Wickham Market Parish Council

Bring Your Own Device (BYOD) Agreement Form

Name: _____
Role: Councillor / Clerk / Staff / Contractor (circle one)
Email Address (Council-Issued): _____

Agreement

By signing this form, I agree that when using my personal device for council business:

1. I will use only my council-issued email address for all council communications.
2. My device will have up-to-date security patches and operating system updates.
3. I will maintain a secure unlock method (password, PIN or biometrics).
4. I will ensure council data is not stored in personal cloud storage unless permitted.
5. I will immediately report any loss, theft or suspected security breach.
6. I understand that failure to comply may result in removal of access to council systems.
7. I will delete all council information if I leave the council or no longer require access.
8. I understand that this is required as part of the council's compliance with Assertion 10. [Document | Word]

Signature: _____
Date: _____

3. Quick-Reference Checklist for Councillors and Staff

Daily / Routine Actions

- Use only your council email account.
- Do not forward emails to personal accounts.
- Keep devices locked when unattended.
- Do not store council documents in personal cloud folders.

Monthly Actions

- Check for device updates and install them.
- Review email for items that should be filed or deleted in line with retention schedules.

When Handling Documents

- Store files only in council-approved locations.
- Ensure documents are accessible before publishing.

When Something Goes Wrong

- Report suspicious emails immediately.
- Report lost devices to the Clerk straight away.
- If you accidentally email the wrong person, notify the Clerk as a data breach.