Ottery St Mary Town Council
IT & BYOD Policy (Assertion 10 – Digital & Data Compliance)

**Adopted:** 2nd March 2026 Minute reference C/26/03/16

**Review:** Annually (next review due 12 months after adoption)

## 1. Purpose and Scope

This Policy sets out how councillors, employees, contractors and volunteers must use information technology (IT) and handle Council data when conducting Council business. It applies to use on Council-owned devices and systems and to authorised use of personal devices (BYOD – Bring Your Own Device). It supports compliance with Assertion 10 of the Annual Governance and Accountability Return (AGAR) and paragraph 1.54 of the 2025 Practitioners' Guide (Smaller Authorities Proper Practices Panel), and aligns with the NALC IT Policy template guidance.

## 2. Principles

1. Use Council systems for Council business. Where personal devices are used, they must meet the security controls in this Policy.
2. Protect personal data in line with UK GDPR and the Data Protection Act 2018.
3. Use only Council-owned email addresses for official correspondence (e.g. @otterystmary-tc.gov.uk). No forwarding to personal inboxes.
4. Maintain accessibility, transparency and records in line with statutory duties.

## 3. Roles and Responsibilities

Council: Adopts and reviews this Policy; provides appropriate systems and training.
Town Clerk (RFO): Policy owner; ensures implementation, training, and incident management; oversees DPIAs where required.
Councillors/Staff/Volunteers: Comply with this Policy, complete mandatory training, and report incidents without delay.

IT Support/Processors: Act only on written instructions; implement technical measures; report incidents.

**4. Authorised Systems**

5. Email: Council domain accounts must be used for all Council business. Shared functional mailboxes may be used (e.g., clerk@...).
6. Storage: Council-approved cloud or network storage with managed access and backups. Personal cloud accounts (e.g., personal OneDrive, Dropbox) must not be used for Council data.
7. Messaging/Collaboration: Only Council-approved platforms for meetings, chat and file sharing. No WhatsApp groups for Council business unless expressly authorised with retention controls.

**5. Acceptable Use**

8. Council data must not be copied to unmanaged locations or personal accounts.
9. Do not share accounts or passwords. MFA (multi-factor authentication) must be enabled where available.
10. Do not install unlicensed or unauthorised software.
11. Email: use professional tone; do not send personal data to group lists without need and appropriate controls.

**6. BYOD – Personal Devices for Council Business**

12. Eligibility: BYOD is permitted only where approved by the Clerk and subject to signing the BYOD Agreement.
13. Security Baseline: Devices must have a supported OS, current security updates, full-disk encryption, passcode/biometric lock, and automatic lock (≤5 minutes).
14. MFA: Council accounts accessed on personal devices must use MFA.
15. Separation: Council data must be stored in managed apps/containers where provided (e.g., Microsoft 365 apps with conditional access).
16. Backups: Personal device backups must not upload Council data to personal cloud; use Council-managed storage.
17. Loss/Theft: You must report immediately so remote wipe/lockout can be actioned for Council data.
18. Leavers/Role Change: Access to Council data will be removed; users must return or delete Council data and confirm deletion in writing.

**7. Data Protection & Records**

19. Process personal data lawfully, fairly, and transparently with a clear lawful basis.
20. Use Council email and storage so records can be retained and disclosed when required (FOI/EIR/SAR).
21. Retention: Follow the Council's Document Retention and Disposal Policy. Do not keep data longer than necessary.
22. DPIA: Conduct DPIAs for new systems or high-risk processing.

**8. Information Security Controls**

23. Passwords: minimum 12 characters or passphrase; never reuse across services; change if compromised.
24. Updates: Enable automatic updates for OS and apps.
25. Anti-malware and firewall enabled.
26. Phishing: verify unexpected requests; do not click suspicious links; report immediately.
27. Public Wi-Fi: use secure networks or VPN; never process sensitive data on open Wi-Fi.

**9. Website & Accessibility**

The Council's website will meet WCAG 2.2 AA standards with an up-to-date Accessibility Statement. Documents published online must be produced in accessible formats as far as reasonably practicable.

**10. Incident Reporting**

Report actual or suspected data breaches, cyber incidents, or loss/theft of a device immediately to the Clerk. The Clerk will assess, contain, and, where necessary, notify the ICO and affected individuals within statutory timescales.

**11. Training & Review**

All councillors and staff must complete periodic data protection and cyber awareness training. This Policy will be reviewed annually or sooner following incidents, audits, or changes in law or guidance.

**12. Enforcement**

Breaches may lead to withdrawal of access, disciplinary action (for staff), standards referrals (for members), and/or reporting to relevant authorities. Serious or repeated breaches may result in termination of BYOD permission.

**13. Related Documents**
Data Protection Policy; Privacy Notices; Records Retention Policy; FOI/EIR Policy; Email and Communications Policy; Social Media Policy; Business Continuity Plan.

**14. Policy Ownership**
Owner: Town Clerk (RFO). Queries to: clerk@otterystmary- tc.gov.uk