Andover Town Council

IT, Email & Digital Governance Policy

Version 1.0 – March 2026

1. Purpose

This policy sets out how Andover Town Council manages its IT systems, email communication, digital services, data, and online presence to ensure compliance with:

- **Assertion 10 – Digital and Data Compliance** (2025 Practitioners' Guide)
- **UK GDPR & Data Protection Act 2018**
- **Freedom of Information Act 2000 & Transparency Code**
- **Website Accessibility Regulations (WCAG 2.2 AA)**

It complements (but does not replace) the Council's **Data Protection Policy**.

2. Scope

This policy applies to:

- Employees
- Councillors
- Contractors, volunteers, and temporary staff
- All devices used for Council business (Council-owned or personal)

3. Council-Owned Domain and Email Use

3.1 Mandatory Use of Council Email

All Council business **must** be conducted using a Council-owned domain email account (e.g. name@andover-tc.gov.uk).
Assertion 10 explicitly prohibits free email services such as Gmail, Yahoo or Outlook for official work.

3.2 Prohibited Email Use

The following must **not** be used for Council work:

- Gmail

- Hotmail/Outlook.com
- Yahoo
- iCloud
- Personal email accounts in any format

3.3 Security Requirements

- Strong passwords must be used on all accounts.
- Multi-factor authentication (MFA) is required where available.
- Lost credentials must be reported immediately.

4. IT Equipment and Usage Rules

4.1 Use of Devices

Staff and councillors may use:

- **Council-owned devices** (preferred)
- **Personal devices**, only if secured and approved

All devices used for Council work must follow identical security standards.

4.2 Minimum Security Requirements

All devices must have:

- Up-to-date antivirus software
- Regularly applied security updates
- Screen lock and password protection
- Encrypted storage (where possible)
- No unauthorised software installed

4.3 Backups

Digital records must be backed up regularly using Council-approved systems.

4.4 Cybersecurity Training

Training in safe IT use, GDPR, and FOI must be completed and refreshed annually.

5. Website Governance

5.1 Accessibility Compliance

The Council has a website compliant with:

- **WCAG 2.2 AA** accessibility standards

5.2 Publication Requirements

The website includes:

- FOI Publication Scheme
- Transparency Code information
- Agendas, minutes, budgets, policies
- An up-to-date accessibility statement

5.3 Ongoing Monitoring

The website is regularly reviewed for:

- Broken links
- Missing documents
- Accessibility issues
- Outdated information

6. Data Protection Responsibilities

The Council:

- Maintains a **Record of Processing Activities (ROPA) – in progress**
- Conducts DPIAs where required
- Reviews and enforces data retention schedules
- Ensures secure storage and destruction of personal data

All personal data processing must comply with UK GDPR and DPA 2018.

7. Freedom of Information (FOI) and Information Governance

The Council maintains:

- An FOI Policy
- Clear FOI and EIR request handling procedures

- A disclosure log

Requests must be handled within statutory deadlines:

- **20 working days for FOI**
- **40 working days for EIR**

8. Breach Reporting

Any suspected or actual data breach must be immediately reported to the **Clerk** and **Data Protection Officer**.

The Council will:

- Investigate breaches
- Maintain an incident log
- Report notifiable breaches to the ICO

9. Record-Keeping and Audit

To meet Assertion 10, the Council maintains:

- Evidence of annual IT and GDPR training
- Website compliance checks – done by our website provide.
- Email domain management records
- Logs of requests (FOI, SAR, etc.)
- Internal audit trail confirming compliance

10. Enforcement

Failure to comply with this policy may result in:

- Loss of IT access
- Withdrawal of permissions to use personal devices
- Disciplinary action (for staff)
- Code of Conduct referrals (for councillors)

11. Review

This policy will be reviewed annually and before approval of each AGAR to ensure compliance with Assertion 10.