



# IT Acceptable Use & Governance Policy

New Policy - This policy provides a single, clear framework for the safe, secure, and responsible use of all IT systems at Newton Abbot Town Council.

A unifying document that sits above and cross-references all existing NATC IT policies including - Internet & Email, Password, Remote Access, Firewall, GDPR, and the AI Policy and incorporates the SAPP (Smaller Authorities Proper Practices) template.

It is also a requirement of the AGAR Assertion 10 compliance.

Date of adoption	Full Council 3 <sup>rd</sup> June 2026, Minute number 26/06( )
Reviewed	
Next Review Date	As required
Reviewed By	Policy & Resources Committee 17 <sup>th</sup> June 2026

# IT Acceptable Use & Governance Policy

## 1. Purpose

This policy provides a single, clear framework for the safe, secure, and responsible use of all IT systems at Newton Abbot Town Council.

It acts as the primary user-facing policy, setting out expected behaviours and governance principles while directing users to detailed supporting policies.

This policy does not replace existing policies, It unifies and governs them.

## 2. Scope

This policy applies to:

- Councillors
- Employees
- Contractors
- Volunteers
- Third parties with authorised access

It covers all Council IT systems, including:

- Devices and equipment
- Networks and infrastructure
- Email and internet services
- Data and information systems
- Cloud and remote access systems
- Artificial Intelligence tools

## 3. Governance Structure

This policy sits at the top of the Council's IT governance framework - structure:

- Level 1. This policy. IT Acceptable Use & Governance
- Level 2. Supporting IT policies
- Level 3. Technical controls and procedures

All users must comply with this policy and all linked policies such as Internet & Email, Password, Remote Access, Firewall, GDPR, and the new AI Policy

## 4. Core Principles

All users must:

- Act lawfully and in the public interest
- Protect Council systems, data, and reputation
- Maintain confidentiality, integrity, and availability of information
- Follow security best practices at all times
- Exercise professional judgement and accountability

Users remain responsible for their actions, including work supported by digital tools or AI.

## 5. Acceptable Use

Council IT systems are provided for official use.

You must:

- Use systems for legitimate Council business
- Maintain professional standards in all communications
- Follow all relevant policies and procedures

You must not:

- Misuse systems or data
- Access inappropriate or unlawful content
- Install unauthorised software
- Circumvent security controls

See Internet and Email Policy

## 6. Identity, Access and Passwords

You must:

- Use strong, unique passwords
- Keep login details secure
- Use multi-factor authentication where available

You must not:

- Share passwords
- Reuse passwords across systems
- Disclose credentials via email or phone

See Password Policy

## **7. Devices and Remote Working**

You must:

- Only use approved devices and systems
- Keep devices updated and secure
- Protect devices from loss or unauthorised access

Where using personal devices (BYOD):

- Apply the same security standards as Council devices
- Ensure secure storage of Council data

See Remote Access and Mobile Working Policy

## **8. Network Security**

The Council maintains secure network infrastructure to protect systems and data.

You must:

- Use networks responsibly
- Not attempt to bypass security controls
- Report any suspected vulnerabilities

See Firewall Policy

## **9. Data Protection and Information Governance**

You must:

- Handle all personal and sensitive data lawfully
- Only access data necessary for your role
- Store and share data securely
- Follow retention and disposal requirements

You must not:

- Disclose confidential information without authority
- Use unauthorised systems to process Council data

See GDPR Data Protection and Privacy Policy

## **10. Use of Artificial Intelligence (AI)**

AI may be used to support Council work where appropriate.

You must:

- Not input sensitive or confidential data without authorisation
- Verify and check all AI-generated outputs
- Ensure outputs are accurate, lawful, and appropriate

You remain accountable for all outputs.

Detailed rules:

See AI Policy

Source: AI Policy, p.2–3

## **11. Training and Awareness**

You must:

- Complete required IT and cybersecurity training
- Stay aware of current risks such as phishing
- Apply training in daily work

The Council will provide regular training and updates.

## **12. Incident Reporting**

You must report immediately:

- Data breaches or suspected breaches
- Phishing or suspicious emails
- Lost or stolen devices
- Unauthorised access

Reports must be made to:

- Town Clerk
- IT Service Provider

---

## **13. Monitoring and Compliance**

The Council may:

- Monitor system usage and communications

- Audit compliance with policies
- Access systems where required for legal or operational reasons

Monitoring will comply with legal requirements.

---

#### **14. Enforcement**

Failure to comply may result in:

- Removal of access to systems
- Disciplinary action
- Legal action

Serious breaches may constitute gross misconduct.

---

#### **15. Policy Relationships**

This policy must be read alongside:

- Internet and Email Policy
- Password Policy
- Remote Access and Mobile Working Policy
- Firewall Policy
- GDPR Data Protection and Privacy Policy
- Artificial Intelligence Policy

These documents provide detailed operational and technical requirements.

---

#### **16. Review**

This policy will be reviewed regularly to reflect:

- Legislative changes
  - Cybersecurity risks
  - Technological developments
  - Council operational needs
-