INFORMATION TECHNOLOGY (IT) POLICY

Approved at Full Council March 2026

1. Purpose and Scope

This policy sets out how Tetbury Town Council will use, manage, and protect its information technology (IT) systems and digital assets. It applies to all councillors, employees, volunteers, contractors, and anyone else authorised to access council systems and data.

The policy covers all forms of information and communication technologies including council-owned devices, email systems, websites, cloud storage, third-party platforms, and personal devices used for council business.

This IT Policy should be used alongside the council's other adopted policies and procedures, including but not limited to:

- Data Protection Policy
- Social Media Policy
- Email and Communications Policy
- Information Security Checklist

Together, these documents form the council's approach to responsible digital governance and legal compliance.

---

2. Roles and Responsibilities

- **The CEO** is responsible for managing and enforcing this policy, ensuring IT resources are used appropriately and securely.
- **Councillors and staff** are responsible for complying with the policy and reporting any breaches or incidents immediately.
- External **IT support providers** and contractors must adhere to the standards set out in this policy when handling council information

---

3. Acceptable Use

IT systems and council-issued devices must only be used for legitimate council business. Personal use is discouraged and, where permitted, must not interfere with work responsibilities or compromise the council's security or reputation.

The use of personal email accounts for council business is prohibited. All council correspondence must be conducted through official council email addresses.

Tetbury Town Council
The Old Courthouse
63 Long Street
Tetbury
Glos GL8 8AA
01666 504670 (9.30am – 2.30pm)

4. Data Security and Confidentiality

All devices used to access council data must be password-protected. Where possible, two-factor authentication should be enabled for cloud-based systems and emails.

Documents containing personal data or sensitive information must be stored securely, preferably in encrypted cloud-based storage. Any transfer of such data must use secure sharing tools.

Staff and councillors must not disclose confidential council information to any unauthorised person, either during or after their term of office or employment.

---

5. Software and Hardware Management

Only authorised software approved by the CEO or IT support provider may be installed on council devices. Regular updates and security patches must be applied.

Obsolete or faulty equipment must be securely wiped before disposal, and hardware must be disposed of in line with environmental regulations.

---

6. Email and Communication Standards

All official communications must use the council's designated email system. Emails must be professional, respectful, and concise, and must not contain defamatory or offensive material.

Email accounts must include the standard disclaimer as shown below regarding data protection and information requests.

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, please notify the system manager at ceo@tetbury.gov.uk

You should not use, disclose, distribute, copy or print the email or any information attached to or contained in it. The Council does not guarantee the accuracy or reliability of information in the message.

The views expressed herein are not necessarily those of the Council.

Email records must be retained in line with the council's document retention policy.

---

7. Website and Social Media Governance

The council's website and any official social media accounts are managed by the CEO or designated officers, who are responsible for ensuring published content is accurate, lawful, and regularly updated.

Websites must comply with the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018 and publish a valid accessibility statement.

Any comments received via social media must be moderated in line with the council's social media Policy.

---

8. Remote Working and Mobile Devices

Staff and councillors working remotely must ensure they use a secure internet connection and do not leave devices unattended in public or shared spaces.

Devices must be locked when not in use and must not be shared with family members or others.

Council documents must not be downloaded onto personal devices unless approved by the CEO.

---

9. Incident Reporting and Cyber Security

Any data breach, loss of equipment, or suspected cyber incident must be reported immediately to the CEO, who will investigate and determine whether the breach needs to be reported to the Information Commissioner's Office (ICO).

The council will follow procedures outlined in its Data Protection Policy and maintain an incident log.

All councillors and staff must remain vigilant against phishing attempts and other online threats.

---

10. Training and Awareness

All new councillors and employees will receive IT and data protection training during induction. Periodic refresher training will be offered to all users.

Staff and councillors are encouraged to familiarise themselves with National Cyber Security Centre (NCSC) guidance on staying safe online.

---

11. Compliance with Legislation

This policy ensures compliance with:

- Local Government Act 1972
- Freedom of Information Act 2000

- Data Protection Act 2018 and the UK General Data Protection Regulation
- Local Audit and Accountability Act 2014
- Public Sector Bodies Accessibility Regulations 2018
- Local Government Transparency Code 2015
- Electronic Communications Act 2000

Council data and IT practices will be reviewed regularly to ensure compliance with these and other relevant regulations.

---

12. Disaster Recovery and Backup

The CEO must ensure that critical council documents and emails are backed up at least weekly using a secure and encrypted cloud-based service. Backup systems should include automatic version control and the ability to restore data in the event of accidental deletion or system failure.

A disaster recovery plan must be maintained and reviewed annually, including defined recovery time objectives (RTOs) and procedures for restoring essential operations.

---

13. Third-party Access and Security Standards

Any contractors or third-party software providers accessing council data or systems must do so under a formal agreement. This agreement must specify minimum cybersecurity standards and ensure compliance with the Data Protection Act 2018.

Access must be limited to the data or systems necessary for their role, logged appropriately, and revoked as soon as work is completed.

---

14. Use of CCTV and Surveillance

Where the council operates CCTV or similar surveillance systems, they will be used solely for the purposes stated at the time of installation (such as crime prevention or public safety).

All systems must comply with the ICO's CCTV Code of Practice. Signs must be clearly displayed in areas under surveillance. Data must be stored securely, retained only for the legally allowed duration, and accessed only by authorised personnel.

---

15. Digital Inclusion and Accessibility

The council recognises the importance of digital inclusion. Support and training will be offered to councillors and staff who are less confident using technology. Residents who are digitally excluded will be offered alternative methods of accessing council information and services, such as paper notices or telephone enquiries.

The council's website and online documents must comply with accessibility regulations and offer downloadable content in accessible formats.

---

16. Review and Monitoring

This policy will be reviewed annually by the CEO and presented to the full council for approval.

Breaches of this policy may result in disciplinary action, reporting to the Monitoring Officer, or other action in line with the council's Code of Conduct or HR procedures.

This policy supports the council's commitment to maintaining high standards of transparency, accountability, and information security.

Tetbury Town Council
The Old Courthouse
63 Long Street
Tetbury
Glos GL8 8AA
01666 504670 (9.30am – 2.30pm)