IT POLICY

YEOVIL TOWN COUNCIL

YEOVIL TOWN COUNCIL

IT POLICY

1. Purpose

1.1 This policy sets out the principles and rules governing the use, management, and security of the Council's information technology (IT) systems and data.

1.2 It aims to:

- Protect Council information assets
- Ensure compliance with legal and regulatory requirements (including UK GDPR and Data Protection Act 2018)
- Promote secure and efficient use of IT resources
- Reduce risks such as cyber incidents and data breaches

2. Scope

2.1 This policy applies to all Councillors, employees, contractors, and volunteers.

2.2 All must comply with its provisions.

2.3 This policy applies to:

- All Council-owned or managed IT systems, devices, and data
- Personal devices used to access Council systems (where permitted)
- All Council-owned mobile devices, including work mobile phones

3. Responsibilities

3.1 **Council**

3.1.1 Ensure appropriate IT systems and security measures are in place

3.1.2 Provide training and guidance on IT use

3.2 **Responsible Officer**

3.2.1 The Chief Executive / Town Clerk acts as the Responsible Officer

3.2.2 Overall responsibility for IT governance and compliance

3.2.3 Ensures policies are implemented and reviewed

3.3 **Users**

3.3.1 All users must:

- Use Council IT systems responsibly and securely
- Follow this policy and associated procedures
- Report any suspected security incidents immediately

3.4 **Councillors**

3.4.1 Councillors will be provided with an official Council email address for the conduct of Council business.

3.4.2 Councillors do not have access to Council IT systems, networks, or data beyond their Council email account unless explicitly authorised.

3.4.3 The Council email account must be the only email account used by Councillors for all Council-related communications, including both sending and receiving emails.

3.4.4 Councillors must not use personal email accounts for Council business.

3.4.5 Councillors must ensure their Council email account is used in a secure and responsible manner in line with this policy.

3.4.6 Failure to comply with the requirement to use Council-issued email addresses for Council business may result in action being taken by the Council, including:

- Withdrawal or restriction of access to Council IT services (including email access)
- Referral to the appropriate Council body (e.g. Standards Committee) where conduct may breach the Councillor Code of Conduct
- Formal notification and requirement to comply with this policy

4. Acceptable Use

4.1 Users must:

- Use IT systems primarily for Council business
- Ensure communications are professional and lawful
- Avoid accessing inappropriate, offensive, or illegal content
- Not install unauthorised software or hardware

4.2 Limited personal use may be permitted where it:

- Does not interfere with work
- Does not incur additional costs or risks
- Complies with this policy

5. Information Security

5.1 Data Protection

5.1.1 All personal data must be handled in accordance with UK GDPR and the Data Protection Policy

5.1.2 Only collect and store data necessary for Council functions

5.1.3 Data must be securely stored and not retained longer than necessary

5.2 Passwords and Access

5.2.1 Strong passwords must be used (minimum 12 characters recommended)

5.2.2 Passwords must not be shared

5.2.3 Multi-factor authentication (MFA) must be used where available and is mandatory for access to Council systems where it is implemented, including all remote access

5.2.4 Access to Council systems will be restricted to authorised users only and granted on a least-privilege basis

5.3 Device Security

5.3.1 Devices (including laptops, tablets, and work mobile phones) must be locked when unattended

5.3.2 Only authorised users may access Council devices

5.3.3 Anti-virus software and updates must be enabled and kept up to date where applicable

5.3.4 Work mobile phones must be secured with a PIN, password, or biometric lock

5.3.5 Where possible, encryption and remote wipe capabilities must be enabled on mobile devices

6. Email and Communications

6.1 Council email accounts must be used for official correspondence

6.2 Users should be cautious of phishing emails and suspicious links

6.3 Confidential information must only be shared securely

6.4 Email retention must follow Council records management policies

6.5 Councillors must use their Council-issued email address exclusively for all Council business and must not use personal email accounts for Council correspondence

6.6 Non-compliance with Council email requirements may be treated as a breach of Council policy and, where applicable, the Councillor Code of Conduct

6.7 Council-issued mobile phones must be used in accordance with this policy, and any Council communications sent from a mobile device must use approved Council systems (e.g. Council email accounts)

7. Internet Use

7.1 Internet access must be used responsibly

7.2 Users must not download illegal or unsafe content

7.3 Council reserves the right to restrict or monitor internet access

8. Remote Working and Mobile Devices

8.1 Remote access to Council systems must be secured using multi-factor authentication (MFA) and will not be permitted without MFA enabled

8.2 Work mobile phones may be used for Council business where authorised and must comply with this policy

8.3 Personal devices must meet minimum security standards if used

8.4 Council data accessed via mobile devices must not be stored locally unless authorised

8.5 Loss or theft of devices (including work mobile phones) containing Council data must be reported immediately

8.6 Mobile Phone Acceptable Use

8.6.1 Work mobile phones are provided for Council business and must be used responsibly and primarily for official purposes

8.6.2 Limited personal use may be permitted where it:

- Does not interfere with Council duties
- Does not incur additional costs to the Council
- Complies with this policy

8.6.3 Users must not:

- Install unauthorised or unsafe applications

- Use devices for illegal, offensive, or inappropriate activities
- Circumvent security controls or monitoring systems

8.6.4 Council data accessed or stored on mobile phones must be:

- Kept secure at all times
- Not shared via unapproved applications or messaging services

8.6.5 When working within Council premises, users must connect work mobile phones to the Council's secure Wi-Fi network where available and approriate, in order to minimise the use of mobile data and manage costs effectively

8.6.6 Users are responsible for:

- Keeping devices physically secure
- Ensuring devices remain operational for Council duties
- Reporting faults, loss, theft, or misuse immediately

8.6.7 The Council reserves the right to:

- Monitor usage in line with legal requirements
- Restrict applications or services
- Recover devices when no longer required or upon termination of role

9. Data Storage and Backup

9.1 Data must be stored on approved cloud of hosted systems

9.2 Regular backups must be maintained

9.3 Users must not store Council data on unauthorised external devices

10. Cyber Security and Incident Reporting

10.1 All suspected incidents (e.g. data breach, phishing attack, lost device) must be reported immediately to the Responsible Officer

10.2 The Council will investigate incidents and take corrective action

10.3 Serious breaches may need to be reported to the Information Commissioner's Office (ICO)

11. Monitoring and Compliance

11.1 The Council may monitor IT use in line with legal requirements

11.2 Breaches of this policy may result in disciplinary action

12. Training

12.1 All users should receive basic IT security training

12.2 Regular awareness updates should be provided

13. Related Policies

13.1 Data Protection Policy

13.2 Data Retention Policy

14. Review

14.1 This policy will be reviewed annually by the Council; or following significant changes in legislation or IT infrastructure.

Yeovil Town Council
September 2026
To be reviewed: September 2027