

Frome Town Council Constitution

Information Technology Policy

Frome Town Hall
Christchurch Street West
Frome
BA11 1EB

01373 465757
info@frometowncouncil.gov.uk
www.frometowncouncil.gov.uk

Date adopted: 27 May 2026
Review Date: May 2028

A copy of this document is also available in different formats such as large print, audio or in a different language, please contact us if we can help you.

Table of Contents

Glossary of abbreviations	3
1. Purpose and Scope.....	3
2. Acceptable Use	3
3. Equipment and Security	3
4. Personal Devices (BYOD)	3
5. Authentication	3
6. Monitoring	4
7. Remote Working.....	4
8. Email and Communications.....	4
9. Internet and Social Media	4
10. Data Protection	4
11. Data Breach Response	4
12. Policy Violations	4
13. Support and Review	4
14. Internet & Email Use Agreement	4
15. Use of Artificial Intelligence (AI) – CoPilot	4
Appendix 1	6

Glossary of abbreviations

FTC	Frome Town Council
AI	Artificial Intelligence
BYOD	Bring your own device
SAR	Subject Access Request
FOI	Freedom of Information
MFA	Multi Factor Authentication
ICO	Information Commissioners Office
RFO	Responsible Finance Officer
GDPR	General Data Protection Regulation

1. Purpose and Scope

This policy sets out rules for use of Frome Town Council (FTC) IT systems to protect data, ensure lawful use, and define responsibilities. Applies to all councillors, staff, contractors, and authorised users across all locations and devices. This policy includes the responsible use of emerging technologies, including Artificial Intelligence (AI).

2. Acceptable Use

FTC systems are for council business. Limited personal use allowed if it does not interfere with work or create risk. Users must lock devices, use authorised systems, and avoid inappropriate or illegal content. Use of Artificial Intelligence (AI) tools must comply with Section 15 of this policy. Users must ensure all AI-assisted work is accurate, appropriate, and properly declared.

3. Equipment and Security

All FTC devices are managed via Azure/Intune and must not be altered. Devices must remain encrypted and secure. Portable devices must be protected, not left unattended, and losses reported immediately.

4. Personal Devices (BYOD)

Personal device use is permitted only via approved systems. Devices must be secure and up to date. Council data must remain protected. Personal devices used for FTC work may be subject to SARs, FOI or legal disclosure.

5. Authentication

Strong passwords must be used and not shared. Multi-Factor Authentication (MFA) is mandatory for all access and must always be used when accessing FTC systems from any non-Intune-managed device.

6. Monitoring

FTC may monitor use of IT systems for security and compliance. Monitoring is proportionate and lawful. Users should not expect full privacy when using council systems.

7. Remote Working

Users must avoid shared devices, use secure Wi-Fi, protect screens and data, and ensure safe handling of documents when working remotely.

8. Email and Communications

Council email must be used for official business. Users must be cautious of phishing and protect sensitive data. Communications may be monitored and disclosed if required. Where AI tools are used to draft communications, their use must be reviewed and disclosed in accordance with Section 15.

9. Internet and Social Media

Use must be lawful and appropriate. Confidential information must not be shared. Personal views must not be presented as council views. AI-generated content must not be shared publicly unless verified, appropriate, and compliant with the council's AI policy.

10. Data Protection

Users must protect personal data, access only what is necessary, and report any breaches immediately. Users must not input personal or sensitive council data into AI tools unless authorised and compliant with data protection requirements (see Section 15).

11. Data Breach Response

All breaches must be reported immediately. FTC will assess, contain, and notify the ICO within 72 hours if required. Failure to report may lead to disciplinary action.

12. Policy Violations

Breaches may result in warnings, loss of access, disciplinary action, termination, or legal action. Serious breaches may be treated as gross misconduct. This includes misuse of AI tools, failure to declare AI-assisted authorship, or entering confidential data into unauthorised systems.

13. Support and Review

Issues must be reported to the Business Manager/RFO or Clerk and if not available, then the Council's IT provider. Policy reviewed every two years.

14. Internet & Email Use Agreement

All staff and Cllrs sign our Internet & Email use policy – attached in Appendix 1.

15. Use of Artificial Intelligence (AI) – CoPilot

15.1 Purpose

The use of Artificial Intelligence (AI) tools (e.g. generative AI, chatbots, automated content tools) must support council business while ensuring accuracy, transparency, security, and compliance with legal obligations including FOI, GDPR, and data protection legislation. For all Council work only the MS CoPilot AI tool available within your MS Business Premium/365 licence should be used.

15.2 Permitted Use

CoPilot may be used by councillors and staff to assist with tasks such as drafting documents, summarising information, research, and idea generation.

15.3 Mandatory Disclosure (Authorship Requirement)

Where AI tools are used to generate or significantly assist in the creation of any document, report, email, or official communication, this must be clearly declared within the document authorship or metadata. Suggested wording: 'This document was produced with the assistance of Artificial Intelligence (AI) tools and reviewed by [Officer/Councillor name]'. Failure to disclose AI-generated content will be considered a breach of this policy.

15.4 Accuracy and Accountability

Users are responsible for verifying the accuracy, legality, and appropriateness of AI-generated content. AI outputs must not be treated as authoritative without human review. Final accountability remains with the named author.

15.5 Data Protection and Confidentiality

No confidential, personal, or sensitive council data may be entered into public AI tools unless explicitly approved and secure.

15.6 Bias and Ethics

AI outputs must be checked for bias, inappropriate language, or misleading content and must not harm the council's reputation.

15.7 Record Keeping and FOI

AI-generated content linked to council business forms part of official records and may be subject to FOI requests, Subject Access Requests, or legal disclosure.

Appendix 1

USE OF INTERNET AND EMAIL

The organisation permits staff to use their terminals to access the Internet and send/receive email for personal/developmental use where necessary.

Staff wishing to use internet/email access for personal/developmental reasons must agree to the following:

- This permission only applies to times OUTSIDE recorded working hours.
- The use of both Internet access and email usage will continue to be subject to the monitoring regime currently in place for work-related traffic.
- Abuse of this permission will be regarded as a disciplinary offence and will be subject to action laid out in the policies on code of conduct and elsewhere.

Abuse of Internet/email access could include but is not exclusively:

- Downloading or distributing obscene, offensive or indecent material
- Using language or behaviour likely to bring Frome Town Council and the organisations it supports, into disrepute
- Using the official role/status of Frome Town Council and/or the organisations it supports, for personal gain
- Using the official role/status of Frome Town Council and/or the organisations it supports, to support a specific political or issue-based campaign
- Using the equipment to contribute to fraud
- Using or passing on privileged or confidential information

The personal use of email or Internet access must be completely in accordance with the range of provisions in the current Code of Conduct

I have read and understood the organisations policy on the use of Internet and email and recognise that to misuse it would be regarded as a disciplinary offence, potentially gross misconduct. I am content to abide by this policy.

Signed:

Print name:

Date: