TODMORDEN TOWN COUNCIL

Information Technology Policy - Computer Equipment, Network, Internet, Email, and Digital Communications

Prepared by: Naomi Crewe, Town Clerk
Date: February 2026
Next Review Date: February 2028

Contents

1. Introduction

1.1 This Information Technology (IT) Policy establishes a clear framework governing the use, management, and security of computer equipment, networks, internet access, email accounts, and digital communication systems provided or supported by the Town Council.

1.2 The Town Council relies on secure and efficient IT systems to support its statutory functions, internal operations, and engagement with residents, partners, and stakeholders.

1.3 This policy seeks to ensure that all IT systems are used effectively, responsibly, lawfully, and in a manner that safeguards Council data and systems from operational, legal, and security risks.

1.4 This policy applies to:

- Employees of the Town Council
- Elected Members using Council issued equipment or accessing Council systems
- Contractors or volunteers who have been granted access to Council IT systems

1.5 All Council issued equipment remains the property of the Town Council and must be returned upon cessation of employment or the end of a Member's term of office.

1.6 Where personal devices are used to access Council systems (including email), device users are responsible for maintaining an adequate level of security, including up-to-date malware protection and secure Wi-Fi access. The Council reserves the right to withdraw access where minimum security standards are not met.

2. Objectives

2.1 Protect the Council, its systems, Employees, Members, and data from risks arising through the use of IT systems, including but not limited to cyber threats, malware, data breaches, or unauthorised access.

2.2 Ensure that Council hardware, software, and data are used appropriately and with due care.

2.3 Minimise disruption to Council business due to avoidable IT security incidents.

2.4 Promote lawful, ethical, and professional use of all IT systems.

3. Cyber and Virus Protection Procedures

3.1 To maintain system security, the following rules apply to all users of Council-provided equipment:

- Unauthorised software, applications, USB drives, external hard drives, and unverified downloads must not be used.

- All software must be scanned using Council-approved antivirus tools.
- Only software licensed or authorised by the Town Council may be installed or used.
- Suspicious emails, attachments, or websites must not be opened and should be reported immediately.

3.2 Users must promptly report any suspected security incident, malware alert, or unusual system behaviour to the Administrative Officer or designated IT provider.

4. Use of Computer Equipment – Employees

4.1 The following conditions apply to Employees using Council equipment:

- Access is limited to authorised personnel only.
- Equipment must be used for legitimate Council business unless limited personal use is explicitly permitted.
- No equipment or software may be removed, copied, or installed without authorisation.
- Unauthorised access or misuse may result in disciplinary action.

5. Use of Computer Equipment – Councillors

5.1 The following conditions apply to Councillors using Council-issued equipment:

- Equipment is provided for Council business and must not be used by unauthorised persons.
- Only authorised and business-related software may be used.
- Equipment must not be altered, modified, or used to install unapproved applications.
- Misuse of equipment may result in a misconduct investigation under the Council's Member Code of Conduct.

6. Use of Printers for Home Working

6.1 Council-issued printers may be used for Council business and reasonable personal use.

6.2 Printer consumables (cartridges, paper) will be provided for Council work. Excessive personal use may result in a contribution being sought.

6.3 Printer faults must be reported to the Administrative Officer for servicing.

7. Email Use

7.1 The Council's email system is provided to support effective communication using Council-provided email addresses that are hosted on the Council's official authority-owned domain.

7.2 All Officers and Members must use their Council-provided email addresses for all official Council business. Personal email accounts must not be used for Council communications.

7.3 Email misuse can result in operational inefficiencies, security risks, and legal liabilities; therefore, all users must comply with the standards set out in this policy.

7.4 Emails sent or received in connection with Council duties constitute Council records and may be subject to disclosure under the Data Protection Act 2018 or the Freedom of Information Act 2000.

7.5 The Council office may access Councillor or Officer email accounts where necessary to fulfil a statutory obligation, including Freedom of Information (FOI) requests, Subject Access Requests, or other legitimate governance or legal requirements. Such access will be carried out only by a senior officer and will be strictly limited to the information required.

7.6 Email account passwords will be held securely by the Town Council office and accessible only to authorised senior officers for operational or legal purposes.

7.7 Councillors and Officers will be notified in advance where access to their Council email account is required, unless doing so would compromise a legal obligation or ongoing investigation.

8. Email Procedures – Authorised Use

8.1 The Council's email system must be used professionally and lawfully. Users must:

- Use clear, respectful, and appropriate language.
- Limit recipients to those who genuinely require the information.
- Verify unfamiliar or suspicious emails before opening attachments.
- Avoid using email where a conversation or meeting is more appropriate.
- Protect confidential information and ensure compliance with data protection legislation.
- Recognise that emails may form legally binding commitments; only authorised Officers may make such commitments on behalf of the Council.

8.2 The following uses are prohibited:

- Bullying, harassment, discriminatory, or offensive communication.
- Excessive personal use, chain emails, or non-business content.
- Sharing or distributing copyrighted or illegal materials.
- Circulating confidential, defamatory, or inappropriate content.

9. Email Reporting and Sanctions

9.1 Councillors receiving inappropriate emails from staff should report concerns to the Town Clerk, or to the Chair of the Staffing Committee if the concern relates to the Town Clerk.

9.2 Staff receiving inappropriate emails from colleagues should report concerns to the Town Clerk, or to the Chair of the Staffing Committee if the concern relates to the Town Clerk.

9.3 Staff receiving inappropriate emails from Councillors may raise a grievance or report the issue via the procedures outlined in the Members' Code of Conduct.

10. Internet Use

10.1 Employees and Councillors are encouraged to use the internet for duties related to their role.

10.2 Information published in the Council's name must be accurate, relevant, and authorised.

10.3 Where personal opinions are expressed externally, a clear disclaimer must be included.

10.4 Users must ensure that copyright and intellectual property rights are respected.

10.5 Accessing or distributing offensive, illegal, or non-work-related material using Council systems is strictly prohibited and may result in disciplinary or misconduct proceedings.

11. Internet Procedures – Acceptable and Unacceptable Use

11.1 Acceptable use includes research, communication, and activities directly related to Council business.

11.2 Unacceptable use includes, but is not limited to:

- Accessing harmful or inappropriate websites.
- Posting unauthorised content on social media.
- Downloading or sharing copyrighted or illegal materials.
- Hacking, attempting to bypass security protections, or unauthorised access.
- Defamatory, discriminatory, or threatening communication.
- Password sharing or unauthorised access to another user's account.
- Fraudulent activity or piracy.
- Passing personal views as representing the Council.

11.3 Staff unsure about acceptable use must seek guidance from their line manager.

12. Monitoring – Employees

12.1 The Council reserves the right to monitor email and internet usage to ensure compliance with policies, legal requirements, and security standards.

12.2 Monitoring constitutes personal data processing and will be conducted in line with the Employee Privacy Notice.

12.3 Monitoring data will not be shared with third parties and will be handled in accordance with the Data Protection Act 2018.

12.4 Information obtained may be used in disciplinary procedures where necessary.

13. Use of Social Media and Networking Sites

13.1 Users must not post work-related content, confidential information, or material that could damage the reputation of the Council, colleagues, or residents.

13.2 Councillors and Employees who engage in social media activity for Council business must do so using dedicated, separate Council-related accounts. Personal social media accounts must not be used for official Council communications, representation, or public engagement on Council matters.

13.3 Council-designated social media accounts must be managed in accordance with the Council's Communications Policy, with access granted only to authorised users.

13.4 Work-related social media activity is only permitted when authorised as part of the Council's communications strategy.

13.5 Employees must not access social media for personal use during working hours except during agreed break times.

14. Intellectual Property Rights

14.1 Intellectual property produced by Employees in the course of their duties belongs to the Town Council.

14.2 This includes copyright, patents, trademarks, design rights, and related protections.

14.3 Employees waive all moral rights relating to such work and must support the Council in securing appropriate protections.

15. Network and System Security

15.1 Any security concerns must be reported immediately to the Administrative Officer or the Council's designated IT provider. Prompt reporting ensures timely mitigation of potential threats.

15.2 Users must not attempt to bypass, disable, or interfere with security controls, including firewalls, antivirus software, intrusion detection systems, or network access restrictions.

15.3 All Council-issued email accounts and systems must be accessed using Council-provided passwords, which will be held securely by the office and senior officers as required.
15.4 Remote access to Council systems must be conducted only via secure, Council-approved methods (e.g., VPN, encrypted connections).

15.5 All portable devices (laptops, tablets, mobile phones) must be encrypted and secured against loss, theft, or unauthorised access.

15.6 Users must ensure that software updates, security patches, and antivirus definitions are applied promptly to maintain system integrity.

15.7 Any attempt to gain unauthorised access to Council systems, data, or networks will be treated as a serious breach and may result in disciplinary action, legal proceedings, or both.

15.8 Regular audits and vulnerability assessments may be conducted to ensure compliance with this policy and to maintain the security of Council IT systems.

16. Policy Compliance

16.1 All employees, councillors, contractors, and volunteers are expected to comply fully with this policy. Failure to adhere to these provisions may result in disciplinary action, removal of access privileges, or other sanctions as deemed appropriate by the Council.

16.2 Any questions regarding the interpretation or application of this policy should be directed to the Town Clerk or Administrative Officer.

16.3 This policy will be reviewed at least every two years or more frequently if required due to legislative, technological, or operational changes.