



EMERSONS GREEN TOWN COUNCIL

Social Media, IT and Cyber Security Policy

Date approved: 2nd July 2026

Approved by: Finance and Partnership Committee

Next Review date: July 2029 (Subject to Changes in Legislation)

Contents

1. Introduction
2. Scope
3. Core Principles
4. Acceptable Behaviour and Conduct
5. Social Media Use
6. IT System Use
7. Email and Internet Use
8. IT and Cyber Security
9. Devices and Equipment
10. Remote Working and Off-Site Use
11. Data Protection and Legal Compliance
12. Monitoring and Privacy
13. Risk Awareness and Incident Reporting
14. Training and Support
15. Roles and Responsibilities
16. Monitoring, Misuse and Enforcement
17. Monitoring and Review

1. Introduction

This policy combines and strengthens the requirements of Emersons Green Town Council's previous Social Media Guide, IT and Cyber Security Policy and Information Technology Policy.

It provides a single comprehensive, and operational framework governing the acceptable use of social media, IT systems, email, internet access, remote working, equipment handling and data security.

All employees, members and users share responsibility for protecting the Council's reputation, information, systems, and ensuring legal compliance at all times.

All digital activity must:

- Be secure
- Be professional
- Be lawful
- Be accountable
- Protect the Council's reputation, systems, and data

2. Scope

This policy applies to:

- Employees, Councillors, volunteers, and contractors
- All Council-owned devices, systems, and networks
- Personal devices when accessing Council systems
- Email, internet, social media, and all digital communications
- Remote, mobile, and home working arrangements

3. Core Principles

Users must:

- Act responsibly, respectfully, and professionally at all times
- Protect Council data, systems, and assets from unauthorised access
- Comply with Data Protection, GDPR, copyright, and relevant legislation
- Maintain a clear distinction between personal and official communication
- Protect the Council's reputation and integrity
- Remain vigilant to cyber threats and report concerns immediately

4. Acceptable Behaviour and Conduct

- Online behaviour must reflect the same standards as offline conduct

- Offensive, defamatory, bullying, or inappropriate content is strictly prohibited
- Users must not engage in behaviour likely to cause harm, distress, or reputational damage
- Accessing inappropriate, illegal, or harmful content using Council systems is prohibited
- Any misuse of IT systems or social media may result in disciplinary action, including dismissal

5. Social Media Use

Personal Use:

- Users must clearly state when opinions are personal
- Disclaimers should be used where appropriate
- Users must not bring the Council into disrepute
- Care must be taken when sharing personal or sensitive information

Official Use:

- All Council social media accounts must be approved by the Town Clerk
- Accounts must be operated only by authorised officers
- Content must be accurate, respectful, non-political, and appropriate
- Anonymous posting is not permitted

Representation and Media:

- Users must be transparent when posting on behalf of the Council. All communication must be approved by the Town Clerk or a nominated officer.
- Media enquiries must be referred to the Town Clerk before responding

6. IT System Use

- IT systems must be used primarily for Council business
- Limited personal use is permitted but must be reasonable and not impact duties
- Devices must be locked when unattended
- Equipment must not be altered, repaired, or installed with software without approval
- Hardware must be handled with care and protected from damage
- Personal use should be restricted to break times where possible

7. Internet Use

Email:

- Council email must be used for all Council business
- Personal use must be limited and must not interfere with duties
- Emails must not contain offensive, defamatory, or inappropriate material
- Users must exercise caution with links, attachments, and unknown senders
- Suspicious emails must be reported immediately

Internet Use:

- Internet use must support Council duties
- Access to inappropriate, illegal, or harmful content is prohibited
- Copyright laws must be followed when downloading or sharing material
- Information sourced online must be verified for accuracy before use

8. IT and Cyber Security

Security Measures:

- Devices must be password protected and locked when unattended
- Strong passwords must be used (e.g. three random words)
- Multi-factor authentication (MFA) should be enabled wherever possible
- Antivirus and security software must remain active and up to date

Password Management:

- Default passwords must be changed immediately upon setup
- Passwords must not be shared or written down in insecure locations
- Passwords must be stored securely using approved systems
- Administrative/system access must be strictly controlled and auditable
- Suspected password compromise must be reported immediately

9. Devices and Equipment

General Equipment Use:

- All equipment must be treated with care and maintained appropriately
- Users must not install unauthorised software or hardware
- Equipment must not be dismantled or modified without authorisation

Portable Devices:

- Must be encrypted or protected with strong passcodes
- Must not be left unattended in public places or vehicles
- Must be securely stored when travelling or working remotely
- Loss or theft must be reported immediately

Personal Devices:

- Must meet Council security standards before accessing systems
- Must be updated with latest security patches
- Must be protected with strong passwords or biometric controls
- Council data must be kept separate from personal data
- Only Council email accounts must be used for Council communications
- Devices must not allow unauthorised access by others

10. Remote Working and Off-Site Use

- Access to Council systems must be secure and authorised
- Public or shared computers must not be used unless secure and approved
- Screens must be positioned to prevent unauthorised viewing
- Confidential data must not be visible in public environments
- Devices, files, and papers must not be left unattended
- Sensitive data must be encrypted and handled securely
- Printed documents must be stored securely and disposed of confidentially

11. Data Protection and Legal Compliance

- All users must comply with the Data Protection & Retention Policy
- Council data includes emails, documents, social media content, and communications
- Information may be subject to Freedom of Information (FOI) requests
- Copyright, confidentiality, and intellectual property laws must be adhered to

12. Monitoring and Privacy

- The Council reserves the right to monitor system usage, email, and internet activity
- Monitoring will be lawful, proportionate, and compliant with data protection legislation
- Monitoring data may be used for security, compliance, and investigations
- Logs and records may be retained for audit and legal purposes

13. Risk Awareness and Incident Reporting

- Users must remain vigilant to phishing, scams, and cyber threats
- Incidents (including lost devices, breaches, or suspicious activity) must be reported immediately to the Town Clerk
- Failure to report risks may constitute a breach of this policy

14. Training and Support

- Users will receive appropriate training based on their role
- Additional guidance must be sought where uncertainty exists

15. Role and Responsibilities

Town Clerk:

- Approves systems, social media, and governance controls
- Oversees implementation and compliance
- Ensure compliance within teams
- Provide service-specific instructions

Users:

- Comply with this policy
- Protect Council systems, devices, and data
- Report risks and incidents without delay

16. Monitoring, Misuse and Enforcement

- Systems are monitored for misuse and security risks
- Misuse includes:
 - Accessing inappropriate or illegal content
 - Sending offensive or defamatory communications
 - Unauthorised access, alteration, or sharing of data
 - Introducing malware or security vulnerabilities
 - Excessive personal use affecting work performance
- Breaches may result in disciplinary action and/or legal consequences

17. Monitoring and Review

This policy will be reviewed regularly and updated as required due to operational or legal changes.

The latest version will always be available on the Council website - [Council Policies & Key Documents - Emersons Green Town Council](#)