

Polegate Town Council

POLEGATE



IT POLICY

Policy Number 05		
Issue No.	Date completed	Details of amendments
1	04.06.13	Changes on website
2	23.05.16	Adopted at Annual Stat Meeting
3	22.05.17	Adopted at Annual Stat Meeting
4	21.05.18	Adopted at Annual Stat Meeting
5	20.05.19	Adopted at Annual Stat Meeting
6	05.05.21	Adopted at Annual Stat Meeting
7	16.05.22	Adopted at Annual Stat Meeting
8	22.05.23	Adopted at Annual Stat Meeting
9	20.05.24	Adopted at Annual Stat Meeting
10	19.05.25	Adopted at Annual Stat Meeting
11	11.05.26	Adopted at Annual Stat Meeting

1. Introduction

- 1.1 Polegate Town Council recognises the increasing role of electronic communications and internet access in the modern workplace. These tools offer significant advantages in supporting the Council's business, operations, and communications, but they also introduce risks that must be carefully managed.
- 1.2 To ensure the effective and secure use of information technology (IT) and email, this policy outlines the guidelines and responsibilities for the appropriate use of IT resources by council members, employees, volunteers, and contractors.
- 1.3 Establishing a clear framework is in the best interest of both the Council and its personnel, helping to safeguard data, maintain professional standards and reduce the risk of misuse.

2. Scope

- 2.1 This policy applies to all individuals who use Polegate Town Council's IT resources, including computers, networks, software, devices, date and email accounts. It covers council members, employees, volunteers, and contractors, and applies to both Council-owned equipment and authorised personal devices used for Council business.
- 2.2 All members of staff are required to read and comply with the conditions of this policy regarding the use of information technology, including all computers and mobile devices.

3. Definitions

Offensive email means any email communication that a reasonable person would consider insulting, abusive, degrading, discriminatory, harassing, threatening, or otherwise inappropriate in a workplace context. This includes content that is likely to cause distress or humiliation to the recipient or others who may reasonably view the message, having regard to the content, tone, intent, and circumstances in which it was sent.

Offensive content includes, but is not limited to:

- Discriminatory language relating to protected characteristics (e.g. race, sex, disability, religion, sexual orientation, age, gender reassignment).
- Harassing or bullying language, including repeated unwanted communications
- Sexually explicit, indecent, or obscene material
- Threatening, aggressive, or intimidating language
- Derogatory remarks, slurs, or personal insults
- Content intended to cause distress, alarm or humiliation

- Material that breaches the organisation's dignity at work, equality, or anti-harassment policies

4. Acceptable use of IT resources and email

4.1 Polegate Town Council IT resources and email accounts are to be used primarily for official council-related activities and tasks. Reasonable personal use is permitted, provided it does not interfere with work responsibilities, incur costs to the Council, or violate any part of this policy. Abuse of this privilege may result in its withdrawal.

4.2 Staff are expected to use technology in a courteous, reasonable, and responsible manner. The following activities are strictly prohibited and may result in disciplinary action, including potential dismissal for gross misconduct:

- Receiving, sending, or displaying offensive messages or images
- Using obscene or inappropriate language
- Improper use of email
- Damaging or interfering with computers, systems, or networks
- Violating copyright or intellectual property laws
- Using others' passwords or identities without authorisation
- Accessing or modifying others' folders, work, or files
- Intentionally wasting system resources
- Using Council systems for commercial or illegal activities
- Downloading unauthorised or commercial software
- Accessing chat rooms or gaming platforms on Council devices

5. Device and Software usage

5.1 Where possible, authorised devices, software, and applications will be provided by Polegate Town Council for work-related tasks. Staff must not install, uninstall, delete, or modify any software or settings on Council devices without express permission from the Town Clerk or Town Council.

5.2 All data disks or external media must be virus-checked before use. The Council uses antivirus software to maintain system security.

6. Data management and security

6.1 All sensitive and confidential Polegate Town Council data must be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods must be used when necessary.

6.2 Staff must immediately report any of the following to the Town Clerk or designated IT contact:

- Suspected data breaches or unauthorised access to Council systems or information
- Loss or theft of devices containing Council data
- Suspicious emails, attachments, or links that may indicate phishing or malware
- Discovery of inappropriate, offensive, or suspect material stored on Council systems or devices
- Any unusual system behaviour that may suggest a security issue or compromise

6.3 Prompt reporting ensures swift investigation and resolution, protecting both Council data and users.

7. Network and Internet usage.

7.1 Council network and internet connections must be used responsibly and primarily for official purposes. Accessing professional information via email or websites is permitted where relevant to the role. The Council encourages electronic communications with local, national, and international organisations.

7.2 The Council cannot guarantee the accuracy or content of information gathered online and is not responsible for external content. Security is maintained through appropriate software, internal settings, and password protection.

8. Email Communication

8.1 Email accounts provided by Polegate Town Council are for official communication only. Emails should be in a professional and respectful tone.

8.2 Confidential or sensitive information must not be sent via email unless it is encrypted. Staff must be cautious with attachments and links to avoid phishing and malware. Users should verify the source before opening any attachments or clicking on links.

9. Password and account security

9.1 Polegate Town Council users are responsible for maintain the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

10. Mobile devices and remote work

10.1 Mobile devices provided by Polegate Town Council should be secured with passcodes and/ or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

11. Email monitoring

- 11.1 Polegate Town Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with Data Protection Act and GDPR.

12. Retention and archiving

- 12.1 Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

13. Reporting security incidents

- 13.1 All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

14. Training and awareness

- 14.1 Polegate Town Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates.
- 14.2 All employees and councillors will receive regular training on email security and best practices.

15. Compliance and consequences

- 15.1 Breach of this IT Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

16. Policy Review

- 16.1 This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

17. Contacts

- 17.1 For IT-related enquiries or assistance, users should contact the Town Clerk. Any concerns about this policy should be raised with the Town Clerk in the first instance and may be referred to the Personnel Committee or Town Council if necessary.
- 17.2 All staff and Councillor are responsible for the safety and security of Polegate Town Council's IT and email systems. By adhering to this policy, the Council aims to maintain a secure and efficient IT environment that supports its mission and goals.

**Statement prepared for adoption by Polegate Town Council at its meeting on
11.05.26**

Signed by

Mayor of Polegate

Town Clerk/Proper Office/RFO

I have read the policy and agree to abide by it.

Signed:

Print name:

Date: