



# SEAMER PARISH COUNCIL

www.seamercrossgates-pc.gov.uk

## IT POLICY

Adopted by the Council on 9 September 2025

Next Review due 31 October 2026

### Introduction

1. The Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.
2. This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by Council members, employees, volunteers, and contractors.
3. It is informed by the Smaller Authorities Proper Practices Panel Practitioners' Guide 2025.

### Scope

4. This policy applies to all individuals who use the Council's IT resources, including computers, networks, software, devices, data, and email accounts.

### Acceptable use of IT resources and email

5. The Council's IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

### Device and software usage

6. Authorised devices, software, applications and Council e-mail addresses will be provided by the Council to employees for council-related tasks.
7. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.
8. Council e-mail addresses will be provided to Members of the Council for council-related tasks.

### Data management and security

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

### Network and internet usage

10. The Council does not operate a network.

11. Internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

### **Email communication**

12. Email accounts provided by the Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.
13. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

### **Password and account security**

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

### **Mobile devices and remote Work**

15. Mobile devices provided by the 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.

### **Email monitoring**

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

### **Retention and archiving**

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

### **Reporting security incidents**

18. All suspected security breaches or incidents, including email-related security breaches or incidents, should be reported immediately to the Clerk for investigation and resolution with the Council's IT Support and Website & E-mail providers.
19. Any security breaches or incidents, including email-related security breaches or incidents involving the Clerk should be investigated and resolved with the Council's IT Support and Website & E-mail providers, and the Chairman & Vice-Chairman informed with evidence of this.

### **Training and awareness**

20. The Council will provide all employees and Members with access to training and resources to educate users about IT security best practices, privacy concerns, technology updates and email security and best practices.

### **Compliance and consequences**

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

