SEAMER PARISH COUNCIL

www.seamercrossgates-pc.gov.uk

IT POLICY

Adopted by the Council on 13 October 2026

Next Review due 31 October 2027

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 2026/27.

Scope

4. This policy applies to all individuals who use IT resources, including computers, networks, software, devices, data, and email accounts. The Council acknowledges that the clerk and members use their own personal devices. Everyone must adhere to this policy to maintain digital security.

Training and awareness

5. 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, including:

    i. Yorkshire Local Councils Associations (YLCA) training.

    ii. the National Cyber Security Centre's

        1. Cyber Security training for small organisations https://www.ncsc.gov.uk/training/cyber-security-for-small-organisations-scorm-v2/scormcontent/index.html#/

           and

        2. free Cyber Action Toolkit https://cybertoolkit.service.ncsc.gov.uk/?utm_source=NCSCWebsite&utm_medium=Website&utm_campaign=PublicBeta&_gl=1*1ap9uoy*_ga*MTA3MTI5NDU1OS4xNzU4ODk0ODM1*_ga_FMH2FBTCEP*czE3Njk1OTkxMzEkbzQzJGcwJHQxNzY5NTk5MTMxJGo2MCRsMCRoNTgwMzE3MTY3*_gcl_aw*R0NMLjE3NjE5MjUwMDcuQ2owS0NRand2SkhJQmhDZ0FSSXNBRVFuV2xBQkdkZHVMVUlxWWl0Zmx1ODFjSXkzNkRGNXNXSFYzNHZIRUtQOHBRQmNpdHI0ZjIzZElnNGFBbmNCRUFMd193Y0I.

Acceptable use of IT resources and email

6. The Council's IT resources and email accounts are to be used for official council-related activities and tasks only.

7. When using IT resources for the council's purposes, you must adhere to ethical standards, respect copyright and intellectual property rights, and you must not use equipment or email to access or forward inappropriate or offensive content.

8. An encrypted laptop computer with software and a Council .gov.uk e-mail address will be provided to the clerk by the Council for work-related tasks. The Council acknowledges that the clerk will also operate the Council e-mail on their own personal devices.

9. Council .gov.uk e-mail addresses will be provided to all members by the Council for Council tasks. The Council acknowledges that members will operate the Council e-mail on their own personal devices.

10. If you are using your own device you must make sure you are:

    i. using strong passwords for all your accounts (preferably using a password manager)

    ii. downloading the latest operating system security updates

    iii. using anti-virus software

Network and internet usage

11. The Council does not operate a network.

12. You must be careful about which Wi-Fi networks you join. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. Always make sure you are using a trusted internet connection, which is password protected when carrying out official business.

Password and account security

13. Council users are responsible for maintaining the security of their accounts and passwords.

14. Use the National Cyber Security Centre's advice for choosing a strong password https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words

15. For business continuity, an electronic copy of the clerk's logins and passwords will be held securely by the Chairman. If accessed this must be reported immediately to all Council Members and at the next meeting of the Council.

Email communication

16. Email accounts provided by the Council are for official communication only.

17. You must make sure that emails are professional and respectful in tone.

18. You must always check you are sending any confidential or sensitive information to the correct recipients.

19. Always be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify the source by looking at the email it has come from carefully. Do not download and open anything if you are unsure who has sent it.

Email access

20. The Council reserves the right to check email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. The clerk may need to access emails so that they respond to Freedom of Information or subject-access requests.

21. Personal email accounts are not to be used for council business. If they were they would still be subject to data protections laws and FOI requests.

Data management, data retention and security

22. All sensitive and confidential data should be stored and transmitted securely.

23. You must regularly backup any important data to prevent data loss, and follow the Council's Records Management and Document Retention Policy.

24. Emails should be retained and archived in compliance with the Records Management and Document Retention Policy. Regularly review and delete unnecessary emails to maintain an organised inbox.

Reporting security incidents

25. All suspected security breaches, including email 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.

26. Any security breaches, including email 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.

Compliance and consequences

27. Breach of this IT and Email Policy may result in the suspension of IT privileges.

Policy review

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

Contacts

29. For IT-related enquiries or assistance, users can contact the clerk, who may enlist the assistance of the Council's IT Support and Website & E-mail providers, as necessary.

30. All staff and Councillors are responsible for the safety and security of IT and email systems.

Signed: Chairman of the Council

Clerk of the Council and Responsible Financial Officer

Proper Officer

Date: 13 October 2026