HUNTON PARISH COUNCIL

IT Policy

This policy was adopted by Hunton Parish Council at the meeting held on 19th January 2026.

1. Introduction

1.1 Hunton Parish Council ('the Council') recognises the importance of effective and secure Information Technology (IT) and email usage in supporting its business, operations and communications.

1.2 This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by Council members and the clerk to safeguard IT systems and data and assist in compliance with relevant legislation.

2. Scope

2.1 This policy applies to all individuals (clerk and councillors) who use the Council's IT resources, including computers, software, devices, data and email accounts.

3. Acceptable use of IT resources and email

3.1 The Council IT resources and email accounts are to be used for official Council-related purposes. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy.

3.2 All users must adhere to ethical standards, respect copyright and intellectual property rights and avoid accessing inappropriate or offensive content.

4. Device and software usage

4.1 Where possible, authorised devices, software and applications will be provided by the Council for work-related tasks. Devices will be recorded on the asset register.

4.2 All computers and other devices supplied by the Council must be treated with care at all times, to avoid loss or damage that would have a financial impact on the Council.

4.3 At the end of any period of holding office or employment with the Council, all equipment must be returned to the Chairman in full working condition. If equipment has been lost or damaged, or not returned within 14 days of leaving office, a charge may be made for its replacement or repair.

4.4 Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

5. Data management and security

5.1 All sensitive and confidential Council data should be stored and transmitted securely using approved methods.

5.2 Regular data backups should be performed to prevent data loss. Backups should be stored separately from live systems (off-site or on the Cloud).

6. Internet usage

6.1 The Council's internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

7.1 The clerk and councillors will be given their own email address and account on a domain owned by the Council.

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

7.3 Emails should be professional and respectful in tone and not contain material that could bring the Council into disrepute.

7.4 Councillors should use their Council-provided email account for official business so that Council data remains secure and under Council control. Using personal email should be limited and only when absolutely necessary.

7.5 Any email sent or received in their capacity as clerk or councillor is Council data and may have to be disclosed following requests under the Data Protection Act or Freedom of Information Act. This includes emails on personal accounts when acting as a councillor.

7.6 Confidential or sensitive information must not be sent via email unless it is encrypted.

7.7 To reduce the risk of phishing and malware, users should take the following precautions:

- If an email seems suspicious, do not reply, click links or open attachments.
- Check the sender's email address carefully, not just the display name. Fraudulent emails often imitate familiar names but use incorrect or unusual addresses. Verify the source before opening any attachments or clicking on any links.
- Do not trust urgent or threatening wording as this is often a sign of phishing attempts.

8. Websites and social media

8.1 The clerk will ensure that the Council’s website is regularly reviewed to ensure content is accurate and up to date.

8.2 The Council does not have its own social media accounts, but councillors using social media in their capacity as councillors must make it clear that they are speaking in a personal capacity and not representing the view of the council. They must adhere to the Members’ Code of Conduct.

9. Password and account security

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

9.2 Passwords should be strong and not shared with others.

9.3 Regular password changes are encouraged to enhance security.

9.4 Unattended devices should be password protected.

9.5 Administrative credentials must be stored securely and only be accessible to authorised personnel with a copy provided to the Chairman of the Council in a sealed envelope, to be accessed in an emergency.

10. Mobile devices and secure remote working

10.1 Mobile devices provided by the Council should be secured with passcodes and/or biometric authentication.

10.2 When working remotely, users should follow the same security practices as if they were in the usual work place.

10.3 Do not use public or insecure Wi-Fi for confidential Council business.

10.4 If leaving portable equipment unattended is unavoidable, it must be kept in a locked room or cabinet, or secured in the boot of a car for a short period.

11. Monitoring

11.1 The Council has the right, as an IT provider, to monitor the use of its IT equipment and systems, providing there is a legitimate reason for doing so and the clerk or councillors are informed that such monitoring may take place.

11.2 Any monitoring must be proportionate and comply with relevant data protection and privacy laws.

12. Retention and archiving

12.1 Emails and electronic records should be retained and archived in accordance with legal and regulatory requirements.

12.2 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 clerk for investigation and resolution.

13.2 Where a security breach affects personal data, the Council will follow the Information Commissioner’s Office guidance.

14. Training and awareness

14.1 The clerk will provide councillors with details of any relevant training and resources on IT security best practices, privacy concerns and technology updates.

15. Compliance and consequences

15.1 The Council expects its computer systems and email to be used responsibly. Inappropriate and unauthorised use will be taken seriously.

15.2 Any misuse of Council IT resources by the clerk may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

15.3 Compliance with this policy is part of a councillor’s responsibility and breaches may be dealt with under the Members’ Code of Conduct.

16. Policy review

16.1 This policy will be reviewed every three years to ensure its relevance and effectiveness or when significant guidance changes.