

TERINGTON PARISH COUNCIL

Information Technology Policy (approved March 2026)

1. Introduction

Terrington Parish Council (TPC) recognises the importance of effective and secure information technology (IT) and email usage in supporting the Council's business operations and communications.

This policy sets out the guidelines and responsibilities for the appropriate use of IT resources and email by councillors and officers.

2. Context

TPC does not own or lease any computer hardware or software. It pays for website and email hosting and a TPC domain name and provides councillors and officers with TPC email accounts and maintains a TPC website. Councillors and officers ('users') provide their own hardware and software in conducting TPC business.

3. Security

Access to personal computers, tablets, phones, external hard drives, memory sticks and other devices used for processing or storing TPC data and emails must be protected by strong passwords or biometric authentication. Passwords must not be shared with others and regular password changes are encouraged to enhance security.

Anti-virus and Internet security software must be installed on all machines used for TPC business.

4. Use of email

Email accounts provided by TPC are to be used for Council business only and must be used for all Council business. Personal email accounts should not be used for Council business.

For accountability and transparency reasons, emails should be preserved unless deletion is required by Data Protection legislation.

Users must be cautious before opening attachments to incoming mail and clicking links in mail messages to avoid phishing and malware by carefully verifying the source address of emails and looking for any signs in the wording or content of emails that suggests they are not from a trusted source. Emails identified as spam should be moved to a spam folder.

5. Data management

All sensitive and confidential TPC data such as text documents and spreadsheets must be stored securely on password protected systems and transmitted securely (eg using TPC email).

All data should be backed up to prevent data loss.

In order to ensure the business continuity of TPC, the location and access details of data and files which are necessary for the functioning of TPC should be known to the Chairman and officers in case of the incapacity of one or more of them.

6. Website

TPC must make available and keep up-to-date on its website all documents required by the Transparency Code for Smaller Authorities and all TPC policies.

The TPC website must be accessible to all users and on all platforms and display a Web Accessibility Policy.

The contents of the TPC website may only be changed by the webmaster appointed by the Council.

All material on the TPC website must respect copyright and intellectual property rights and properly attribute material from other sources.

7. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk.

8. Training and awareness

TPC will provide regular training and resources to inform councillors and officers about IT and email security best practice and Data Protection and privacy requirements and legislation.

9. Compliance and consequences

Breach of this IT Policy may result in the suspension of the user's email account and further consequences as deemed appropriate.

10. Policy review

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

11. Contacts

For IT-related enquiries or assistance, users can contact the webmaster or the Parish Clerk.

Date: 9th March 2026

Signature: W M Winning

Role: Chairman of Terrington Parish Council