RIVINGTON PARISH COUNCIL
IT POLICY

Meeting: Full Council

Date Approved: 18TH May 2026

Next review date: May 2027

Version: V1

Contents

1. Introduction

Rivington Parish Council recognises the importance of secure, reliable and effective use of information technology (IT) to support its statutory duties, services, and communications. This policy sets out the standards and expectations for the use of IT systems, equipment, and data to protect the Council, its members, staff, and the community.

2. Purpose

The purpose of this policy is to:

- Ensure IT systems are used lawfully, securely, and efficiently;
- Protect the confidentiality, integrity, and availability of Council information;
- Reduce the risk of cyber security incidents and data breaches;
- Set clear expectations for acceptable and unacceptable use;
- Support compliance with the UK GDPR, Data Protection Act 2018, and other relevant legislation.

3. Scope

This policy applies to all councillors, employees, contractors, volunteers, and any other authorised users who access Rivington Parish Council IT systems, equipment, networks, data, or email accounts, whether working from Council premises, home, or remotely.

4. Acceptable Use

Council IT resources are provided primarily for official Council business. Limited personal use is permitted provided that it:

- Does not interfere with Council duties;
- Does not incur additional cost to the Council;
- Does not breach this policy or any law.

Users must not access, create, store, or distribute material that is illegal, offensive, discriminatory, or could bring the Council into disrepute.

5. Equipment and Devices

- All Council-owned equipment must be used with care and kept secure.
- Devices must be locked when unattended.
- Food and drink should be kept away from IT equipment.
- Equipment must not be altered, repaired, or software installed without authorisation from the Clerk or the Council's IT provider.
- All Council equipment must have appropriate security software installed and maintained.

6. Use of Personal Devices

Use of personal devices to access Council systems or data is permitted only with the approval of the Clerk and subject to appropriate security controls, including password protection and up-to-date software.

7. Data Management and Security

- Council data must be stored only on approved systems and services.
- Personal or sensitive data must be handled in accordance with the Council's Data Protection Policy.
- Data must not be transferred to personal cloud storage or personal email accounts.
- Secure disposal methods must be used when data or equipment is no longer required.

Anti – Virus and Malware Protection

All Council-owned devices, and any personal devices approved for Council use, must have up-to-date anti-virus and anti-malware software installed and enabled. Virus definitions and security updates must be kept current. Users must not disable or bypass protective software. Any suspected malware or virus infection must be reported immediately to the Clerk.

8. Password and Access Control

- Users must use strong, unique passwords and must not share them.
- Multi-Factor Authentication (MFA) should be enabled where available.

- Passwords must be changed immediately if compromise is suspected.

9. Email Usage

- Council email accounts must be used for official business.
- Emails should be professional, accurate, and respectful.
- Users must be vigilant against phishing and malware and must not open suspicious links or attachments.
- Sensitive information should not be sent by email unless appropriate security measures are in place.

10. Internet and Network Use

- Internet access must be used responsibly and primarily for Council business.
- Downloading or sharing copyrighted material without permission is prohibited.
- Users must not attempt to bypass security controls or monitoring systems.

11. Remote Working

When working remotely, users must:

- Ensure screens cannot be overlooked by unauthorised persons;
- Use secure Wi-Fi connections;
- Store Council equipment and documents securely;
- Report any loss or theft of equipment or data immediately.

12. Monitoring

The Council reserves the right to monitor the use of its IT systems, email, and internet access where necessary and proportionate, in line with data protection and investigatory powers legislation.

13. Security Incidents

All suspected or actual IT security incidents, data breaches, or loss of equipment must be reported immediately to the Clerk for investigation and appropriate action.

14. Breaches of Policy

Failure to comply with this policy may result in disciplinary action, withdrawal of IT access, or other action as appropriate.

15. Review

This policy will be reviewed annually, or sooner if required, to ensure it remains effective and up to date.