RUNWELL PARISH COUNCIL

Email: clerk@runwellparishcouncil.gov.uk
Website: www.runwellparishcouncil.gov.uk

IT & DIGITAL COMMUNICATIONS POLICY

Adopted: 2nd March 2026 Minute 185-26/03

1. Introduction

Runwell Parish Council recognises that councillors, staff, and authorised users use a variety of IT systems and digital tools to carry out council business. Each councils IT setup is different, so this policy is designed to provide guidance tailored to Runwell Parish Council while complying with relevant legislation. Councils using external IT providers (including cloud services) must ensure this policy aligns with current practices and contractual arrangements.

2. Purpose

The purpose of this policy is to:

- Set clear expectations for the appropriate use of council IT and digital systems;
- Raise awareness of risks associated with IT use;
- Safeguard council data, equipment, and digital assets;
- Define acceptable and unacceptable behaviour;
- Outline consequences of breaches;
- Clarify rules around limited personal use of council IT equipment (e.g., checking personal email during lunch breaks).

3. Scope

This policy applies to all councillors, staff, and authorised users, whether working in the office, from home, or in any other location. It covers all council-provided IT equipment, software, accounts, and digital communication platforms, including email, messaging apps, social media, and the council website.

4. IT Equipment and Use

4.1 Hardware

- Council equipment is provided for official business. Reasonable personal use is permitted if it does not interfere with council work.
- All equipment must be kept clean, secure, and in good condition. Damage may result in financial liability.
- Do not dismantle or install unauthorised hardware or software.

- USB drives, CDs, or other removable media may only be used with prior approval.
- Report any faults or repairs immediately to the Clerk or IT provider.

4.2 Portable Equipment

- Laptops, tablets, and mobile devices must be stored securely and encrypted when containing council data.
- Smartphones/tablets must use PINs and, where possible, automatic device wipe after failed attempts.
- Equipment must never be left unattended in public or non-council premises unless securely locked.
- Taking photos, videos, or recordings on council premises requires prior permission.

4.3 Personal Devices

- Personal devices may be used to access council systems.
- Devices must have up-to-date antivirus software, use secure connections and store council data separately from personal data.
- Emails must be sent from council accounts; personal addresses must not be used.
- Councillors/staff must report loss, theft, or breaches immediately to the Clerk.
- Removable media must be securely deleted after use.
- Devices must be password-protected, encrypted, and, where possible, set up with automatic lock/wipe features.

5. Health & Safety

- Workstations with screens (VDUs) must meet ergonomic standards.
- Any hazards, including unusual noises from IT equipment, must be reported to the Clerk or IT provider (Cloud Next).

6. Passwords and Authentication

- Strong passwords are mandatory (three random words or equivalent, e.g., PurpleCandleRiver).
- Multi-Factor Authentication (MFA) should be enabled wherever possible.
- The Clerk to make sure administrative credentials are stored securely; List of access codes and passwords are placed in a sealed envelope and are securely stored. In case of an emergency the Chairman can access the location where passwords are stored.
- Passwords must never be shared.

7. Monitoring

- Council systems may be monitored to ensure compliance, detect misuse, and maintain security.
- Monitoring will be proportionate, comply with privacy laws, and logs may be shared internally or with HR/legal advisers as needed.

8. Remote Working

- Extra security measures apply when working away from council premises.
- Sensitive data must be protected using screen filters, secure storage, encryption, and passwords.
- Council data must never be left unattended in public places or vehicles unless securely locked.
- Remote access should use council-provided devices wherever possible; personal devices must comply with section 4.3.

9. Email and Digital Communications

- Use of Council Email and Personal Devices
  Councillors may access and use their Council email accounts on personal phones or devices, provided appropriate security precautions are followed. Council email addresses are to be used for Council business. Councillors must copy the Clerk on all correspondence with external parties conducted on Council business.
- Cyber Security and Safe Use
  Councillors and the Clerk must exercise caution when opening email attachments, clicking links, or downloading files, and must verify sources before accessing content. Personal devices used for Council business must be secured with appropriate passwords, PIN protection, or biometric security.
- Use of Messaging Applications
  WhatsApp or other messaging applications may be used for operational Council business. Any messages relating to Council business must be deleted after one month or when the matter is resolved, whichever is sooner.

  Where a Councillor uses a personal phone or device for Council business, they are personally responsible for ensuring compliance with this requirement. This obligation continues upon resignation or cessation of office.
- Official Record Keeping and Retention
  The Clerk is issued with a Parish Council mobile phone for official Council business. Communications held on this device, and within Council email systems, shall be retained in accordance with the Councils Document Retention Policy.

Councillors are not required to retain Council business communications on personal devices beyond the time limits stated above, as the official record is maintained through the Clerks Council-issued devices and systems.

- Freedom of Information and Legal Status
  Emails are considered as documents under the Freedom of Information Act 2000. Emails, text messages and other digital communications relating to Council business may be subject to Freedom of Information (FOI) requests and shall be treated as official Council records, regardless of the device used.

10. Internet, Copyright, and Data Protection

- Copyright laws must be followed; do not copy material without permission.
- Links or posts must not infringe trademarks or data protection rules.
- Personal or sensitive data must never be uploaded to third-party cloud services without authorisation.
- Only official council social media accounts may be used for council-related posts.

11. Social Media

- Councillors/staff may not post content that could damage the councils reputation.
- Any post referencing the council must clearly state that views are personal unless officially authorised.
- Explicit permission is required to post photos, videos or audio recorded on council premises.
- Councillors/staff are personally liable for online content; breaches may result in disciplinary action or legal consequences.
- Contact from media should be referred to the Clerk.

12. Misuse

- Misuse of council IT or communications systems is taken seriously.
- Breaches may result in disciplinary proceedings, termination of contracts or legal action depending on severity.

13. Policy Review

- This policy will be reviewed on a regular basis or as soon as required by legislation, guidance or council practice.