RYHALL PARISH COUNICL

Bring Your Own Device (BYOD) Policy

1. Purpose

This policy sets out how councillors, employees, and authorised volunteers may use their personal devices to access parish council information and systems. Its aim is to protect personal data, maintain security, and ensure compliance with UK GDPR Relevant provisions in the UK GDPR Articles 5(1)(c), 5(2), 25, 30, 32, 26, 28 and Recitals 39, 78, 82, 83 Data Protection Act and the council's own policies.

2. Scope

This policy applies to:

- Councillors
- Employees
- Contractors or volunteers authorised to access council information
- Any personal device used to access council data, including smartphones, tablets, laptops, and home PCs.

3. Definitions

- **Personal device**: Any device not owned or managed by the parish council.
- **Council data**: Any information created, received, or stored as part of council business, including emails, documents, photographs, and personal data.
- **Access**: Viewing, storing, editing, sending, or receiving council data.

4. Conditions for Use

Personal devices may be used for council business only when:

- The user has read and agreed to this policy.
- The device meets the minimum security requirements (Section 5).
- Access is limited to approved systems (e.g., council email, Microsoft 365, parish council shared folders, parish council WhatsApp group).
- The user understands that council data must remain under council control at all times.

5. Minimum Security Requirements

All personal devices used for council business must have:

- A strong password, PIN, or biometric lock.
- Up-to-date operating system and security patches.
- Up-to-date antivirus/anti-malware protection (where applicable).
- Automatic screen lock after inactivity.

- Encrypted storage
- No shared user accounts with family members or other individuals.

The council may require evidence that these controls are in place.

6. Data Handling Rules

Users must:

- Access council email only through approved secure apps or web portals.
- Store council documents only within approved cloud services (e.g., Zoho)
- Avoid syncing council data to personal cloud services (iCloud, Google Drive, Dropbox).
- Use council-approved communication channels for official business.
- Ensure personal devices are not left unattended in public places.

Users must **not**:

- Forward council data to personal email accounts.
- Use consumer messaging apps (WhatsApp, Facebook Messenger, SMS) for confidential or sensitive council business.
- Store personal data relating to residents outside council systems.

7. Loss, Theft, or Compromise

If a personal device used for council business is lost, stolen, hacked, or otherwise compromised, the user must notify the Clerk **immediately**.

The council may require:

- Remote revocation of access
- Password resets
- A data breach assessment
- Reporting to the ICO if risk to individuals is likely

8. Monitoring and Audit

The council will not access personal content on a user's device. However, it may:

- Audit compliance with this policy
- Require installation of security tools (e.g., multi-factor authentication apps)
- Remove access to council systems if security standards are not met

9. Acceptable Use

Users must ensure that personal devices used for council business:

- Are used responsibly and professionally
- Do not contain illegal or harmful content
- Are not used to harass, bully, or discriminate
- Are not used to conduct council business on insecure networks (e.g., public Wi-Fi without a VPN)

10. Leaving the Council or Ending Access

When a councillor, employee, or volunteer leaves their role or no longer requires access:

- All council data must be deleted from their personal device
- Access to council systems will be revoked
- Any council-issued credentials must be returned or disabled

11. Responsibilities

Users

- Follow this policy
- Maintain device security
- Report incidents promptly
- Protect council data at all times

Parish Council

- Provide secure systems and training
- Maintain records of authorised users
- Review this policy every 2 years
- Investigate breaches and take appropriate action

12. Non-Compliance

Failure to comply with this policy may result in:

- Removal of access
- Formal action under the council's Code of Conduct or employment procedures
- Reporting serious breaches to the ICO

13. Review

This policy will be reviewed in accordance with the Document Review Schedule or sooner if legislation, technology, or council practices change.