WITTON & RIDLINGTON PARISH COUNCIL
Meadowcroft, 40 Cromer Road, Mundesley, Norfolk, NR11 8DB
Tel: 07900 957888. Email: clerk@wittonandridlingtonparishcouncil.gov.uk

Information Technology (IT) Policy

1. Purpose

This policy sets out how Witton and Ridlington Parish Council (the "Council") uses and manages information technology (IT) resources. It aims to:

- Ensure data security and compliance with UK GDPR and the Data Protection Act 2018.
- Protect Council IT systems from misuse, loss, or damage.
- Support councillors, staff, and volunteers in using IT safely and effectively.

2. Scope

This policy applies to all councillors, employees, contractors, and volunteers who use Council IT equipment, systems, or data. It covers:

- Council-owned devices (e.g., laptops, tablets, printers).
- Personal devices used for Council business (Bring Your Own Device – BYOD).
- Council email accounts, websites, and cloud services.
- Access to Council records and data.

3. Acceptable Use

- Council IT resources are provided primarily for Council business. Limited personal use is permitted provided it does not interfere with Council work or breach this policy.
- Users must not access, download, or share illegal, offensive, or inappropriate material.
- Users must not install unauthorised software or applications on Council-owned equipment.
- Copyright and software licensing rules must always be followed.

4. Data Protection & Confidentiality

- All personal data handled by the Council must comply with UK GDPR and the Data Protection Act 2018.
- Sensitive or confidential data must only be accessed by those who need it for Council duties.
- Council data should be stored in secure, approved locations (e.g., OneDrive, SharePoint, or encrypted storage).
- Personal devices used for Council business must have password protection, up-to-date security software, and screen lock enabled.

5. Email & Communications

- Council email accounts must be used for Council business where possible.
- Care must be taken to avoid phishing, spam, and suspicious attachments/links.
- Emails and documents may be subject to Freedom of Information (FOI) requests; professional tone should always be maintained.

6. Cybersecurity

- Strong passwords must be used and changed regularly.
- Multi-factor authentication (MFA) should be enabled where available.
- Anti-virus, firewall, and security updates must be installed promptly.
- Lost or stolen devices must be reported to the Clerk immediately.

7. Remote Working

- Users working from home must ensure their Wi-Fi is password protected.
- Confidential information should not be discussed or displayed in public spaces.
- Council files must only be accessed via approved cloud services or encrypted devices.

8. Social Media & Website

- Only authorised individuals may post on official Council social media accounts or update the website.

- Posts must reflect the Council's official position and avoid political bias, offensive content, or confidential information.

9. Monitoring & Compliance

- The Council reserves the right to monitor IT use for security, compliance, and performance purposes.

- Breaches of this policy may result in disciplinary action, withdrawal of IT access, or referral to relevant authorities.

10. Policy Review

This policy will be reviewed annually by the Parish Council and updated as required to reflect changes in law, technology, or Council operations.

Approved by Witton and Ridlington Parish Council on 12th November 2025

Signed: _____ (Chair/Clerk)

Date of next review: November 2027

IT User Guide – Quick Reference

This guide summarises key rules from the Council's IT Policy. Please follow these at all times when using Council IT systems.

✅ Do's

- Use your Council email for Council business.
- Keep passwords strong, private, and change them regularly.
- Enable Multi-Factor Authentication (MFA) where available.
- Store files only in approved Council systems (e.g., OneDrive/SharePoint).
- Lock your device when unattended.
- Report any lost/stolen devices or suspicious emails to the Clerk immediately.
- Respect confidentiality and GDPR rules.

❌ Don'ts

- Don't use Council IT for illegal, offensive, or inappropriate material.
- Don't share login details with anyone.
- Don't download unapproved software or apps.
- Don't store Council data on personal USB sticks or unencrypted drives.
- Don't post on Council social media unless authorised.
- Don't forward Council emails/documents to personal accounts unless approved.

📧 Email & Communications

- Always be professional – emails may be subject to Freedom of Information (FOI).

- Be alert to phishing scams – check sender addresses carefully.
- Avoid clicking on suspicious links or attachments.

🏠 Remote Working

- Use secure, password-protected Wi-Fi.
- Keep confidential information private (not in public spaces).
- Use approved cloud services to access and share files.

⚠️ **Remember:**
Breach of the IT Policy may result in withdrawal of IT access, disciplinary action, or legal consequences.

For help or reporting issues, contact:

Parish Clerk – clerk@wittonandridlingtonparishcouncil.gov.uk