IT and Digital Use Policy

1. Purpose

The Parish Council recognises that effective and secure use of IT systems and email is essential to support its operations, communications and service to the community.

This policy sets out the rules for using the Parish Council's IT equipment and systems. Its aim is to:

- Ensure the secure and lawful use of IT resources,
- Protect data in line with the UK GDPR,
- Minimise risk while recognising the limited scale and resources of the Council,
- Meet the requirements of Assertion 10 of the Annual Governance and Accountability Return (AGAR), as outlined in the 2025 Practitioners' Guide.

---

2. Who Does This Policy Apply To?

This policy applies to:

- The Parish Clerk (the Council's only employee),
- All councillors when handling Council data or using Council IT systems,
- Any third parties or contractors acting on behalf of the Council.
- Any volunteers working on behalf of the Council, where they access council systems or data

---

3. What Equipment and Systems Are Covered?

This policy applies to all equipment and systems used for Council business, including:

- Council laptop, desktop, mobile phone or tablet,
- Council email and webmail systems,
- Council website and social media,
- Cloud storage solutions (e.g., OneDrive, Google Drive),
- Personal devices used for Council work (Bring Your Own Device – BYOD),
- Telephony used for Council purposes.

---

4. Policy Oversight and Review

The **Parish Clerk** is responsible for:

- Supporting councillors in understanding and following this policy,
- Reporting breaches to the Chair,
- Reviewing the policy annually or as needed in response to guidance or risks.
- Proposing updates to the policy to reflect changes in technology, legislation or emerging security threats.

---

5. Related Policies

This policy should be read in conjunction with:

- The Council's Data Protection Policy,
- The Records Retention Schedule,
- The Code of Conduct,
- Any other relevant HR, disciplinary, or safeguarding policies.

---

6. Monitoring

- Routine monitoring of devices, emails, or internet usage is **not conducted**.
- .
- The Council reserves the right to monitor email and IT usage where legally justified, in accordance with the Data Protection Act 2018 and UK GDPR. Any such monitoring must be authorised and proportionate.
- No CCTV systems are currently in use by the Council.

---

7. Passwords and Security

- Strong passwords (minimum 8 characters including numbers/symbols) must be used.
- Passwords must not be shared, except with the Chair in emergencies.
- Regular password changes are encouraged to enhance account security
- Screens displaying council data must be locked when unattended.
- If password-protected documents are emailed, passwords must be shared via a separate communication method.
- Suspected breaches or compromised passwords must be reported immediately.
- Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

---

8. Use of Equipment

- Council-owned devices must be shut down daily and locked when not in use.
- Key documents must be saved in clearly labelled folders (on cloud or shared drives) to ensure proper backup and access.
- Confidential data must not be stored on unprotected devices or locations.
- Devices must not be left unattended in public areas.

- When working remotely, users must apply the same security principles as when working in the office
- Devices used for Council work should have passcodes or biometric security enabled where available
- Wrose Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy

---

9. Use of Personal Devices (BYOD)

Staff and councillors may use their own devices for Council work only if:

- Devices are password-protected and updated regularly,
- Council email and documents are stored securely and not mixed with personal content,
- Files are not saved permanently on personal devices,
- All council communications are conducted through official channels (e.g., council email).

---

10. Data Protection

- The Council processes personal data in accordance with UK GDPR.
- Personal data must be:
    - Collected and stored securely,
    - Accessed only for valid purposes,
    - Retained only as long as necessary,
    - Disposed of securely (e.g. shredding, secure deletion).
- Data breaches, including loss, theft or compromise of personal data, must be reported to the Clerk immediately and managed in line with the Data Protection Policy.

---

11. Email and Communication

- Council email accounts must be used for all official business.
- Emails must be:
    - Respectful, factual and clear,
    - Free from discriminatory, defamatory or informal content,
    - Not used to commit the Council to any agreement unless properly authorised.
- Personal or sensitive data should not be included in emails unless necessary and secured.
- Be cautious with attachments and links in emails. Do not open attachments or click on links unless you trust the source. Verify unexpected messages before taking action to reduce the risk of phishing or malware

- Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

-

12. Mobile Phones and Text Messaging

- Text messaging may be used for quick factual updates.
- Messages must be respectful and not contain sensitive or confidential data.
- Abbreviations and informal language should be avoided.

---

13. Internet and Software Use

- Internet use on council devices must be limited to business purposes.
- Accessing inappropriate or illegal content is strictly prohibited.
- Only authorised software may be installed on council-owned devices.
- All downloads must be from trusted sources and scanned for viruses.

---

14. Website and Social Media

- Only the Clerk or authorised persons may manage the council's website or social media accounts.
- All content must be factual, non-political, and accessible.
- Council accounts must never be used for personal views.

---

15. Training and Support

- The Clerk will receive basic IT and data protection training as part of their induction.
- Councillors will be briefed on this policy following election/co-option or if the policy is updated.
- The Council will provide ongoing training to staff and councillors as necessary to keep them informed about IT security. Data protection, and emerging risks or technologies.

---

16. Misuse and Disciplinary Action

Examples of misuse include:

- Breaching this policy,
- Installing unapproved software,
- Sharing passwords inappropriately,
- Accessing or sharing offensive or inappropriate content,
- Mishandling personal data,
- Leaving devices unsecured in public.

Such actions may result in:

- Disciplinary procedures (for staff),
- Referral to the Monitoring Officer (for councillors).

In serious cases, IT access may be suspected during investigations to prevent further risk or misuse

Adopted: June 25
Date of Last review: September 25
Next Review Date: September 26