WOOLASTON PARISH COUNCIL

INFORMATION TECHNOLOGY (IT), EMAIL AND DIGITAL COMMUNICATIONS POLICY

1. Introduction
Woolaston Parish Council is committed to ensuring the secure, lawful, and effective use of its information technology (IT) systems. This policy sets out the standards, responsibilities, and procedures for the use of IT equipment, email, and digital communication by councillors, employees, volunteers, and contractors.

2. Scope
This policy applies to all individuals who use the Parish Council's IT resources, including computers, software, mobile devices, data, cloud systems, and email accounts.

3. Acceptable Use of IT Resources and Email
Council IT resources and email accounts must be used primarily for official council business. Limited personal use is permitted provided it:

- Does not interfere with council duties
- Does not breach this policy
- Does not expose the council to security or data protection risks

Users must act ethically, respect copyright and intellectual property rights, and must not access or distribute inappropriate, offensive, or unlawful content.

4. Device and Software Usage, Including Remote Work

Council-issued equipment

- The Clerk will be provided with authorised devices (laptop and printer), software, and applications for work-related tasks.
- Installation of unauthorised or personal software on council devices is prohibited.
- Council devices must be protected with strong passwords and, where available, biometric authentication.
- Devices used outside the office must be stored securely, locked when unattended, protected with antivirus software, and accessible only to authorised users.

Use of personal devices by councillors

- Councillors using personal devices for council business must ensure their devices are secure, updated, and protected against malware or unauthorised access.
- Personal devices must not store council data unless necessary and must be wiped of council information when a councillor leaves office.

5. Data Management and Security

- All sensitive or confidential council data must be stored and transmitted securely using approved methods.
- Regular data backups must be maintained.
- Secure data destruction methods must be used when disposing of old files or equipment.
- "Sensitive data" includes personal data, financial information, legal matters, and any information not intended for public release.

6. Email Communication

- All official correspondence must be sent from council-issued email accounts.
- Routine forwarding of council emails to personal accounts is prohibited due to data protection risks. Forwarding may only occur in exceptional circumstances with proper authorisation.
- Confidential or sensitive information must not be sent by email unless encrypted.
- Users must be vigilant about phishing, suspicious attachments, and unknown links.

7. Password and Account Security

- Users are responsible for keeping their passwords secure and must not share them.
- Passwords must be strong, unique to council systems, and changed regularly.
- Multi-Factor Authentication (MFA) must be used where available.
- Essential data backups must be stored securely.

8. Email Monitoring

The Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant legislation. Any monitoring will be conducted in accordance with the Data Protection Act and GDPR.

9. Social Media and Website Management

The Clerk manages the council's website and official social media (Facebook) account on behalf of the council.

Key requirements

- **Access and passwords** The Clerk must provide login details for all council social media and website accounts to the Chairman to ensure access in the event of absence or emergency.
- **Content standards** All official posts must be:
    - Professional, accurate, and respectful
    - Non-discriminatory
    - Compliant with data protection requirements (e.g., permission required before posting identifiable photos)
    - Free from party-political content
- **Authorised posting** Only the Clerk may post on official council social media accounts or the website.
- **Council property** All accounts, login credentials, and associated content remain the property of the Parish Council. When leaving employment, the Clerk must return all login details and administrative access.
- **Personal social media** Councillors and the Clerk may comment on council matters on personal accounts but must clearly state that views expressed are personal and not official council positions.

10. Home Working (Clerk)

When working from home, the Clerk must ensure:

- Council documents are securely stored and locked away when not in use
- Council equipment is used for work purposes only and not by family members
- A strong, unique password is set on the council laptop
- Electronic files are password-protected and saved to council systems/cloud storage
- Regular backups are maintained
- Login details for essential systems are available to the Chairman for emergency access
- Confidential information cannot be viewed by others in the home
- All council equipment, documents, and data are returned upon leaving employment
- Home Wi-Fi is secured with WPA2/WPA3 encryption

11. Use of Personal Devices by Councillors
Councillors using personal devices for council duties must ensure:

- Devices are protected with a password or PIN
- Council emails are only sent from council email accounts
- Personal email accounts are not used for council business
- All council data is deleted from personal devices when leaving office
- Devices may need to be searched for FOI or legal requests

12. Retention and Archiving
Emails and digital records must be retained in accordance with legal and regulatory requirements (GDPR, DPA, FOI). Users must regularly review and delete unnecessary emails to maintain an organised and compliant system.

13. Reporting Security Incidents
All suspected security breaches or incidents must be reported immediately to the Clerk (designated IT contact). All incidents will be investigated, and appropriate action taken in line with council governance and disciplinary procedures.

14. Training and Awareness
Councillors and staff must maintain awareness of IT security, data protection, and best practice. The Clerk will share relevant guidance from trusted sources such as the ICO, NALC, and GAPTC. Councillors are encouraged to use freely available resources to support their understanding of data protection, cyber security, and transparency obligations.

15. Compliance and Consequences of Misuse
Failure to comply with this policy may result in suspension of IT access and further action as deemed appropriate by the Parish Council.

16. Policy Review
This policy will be reviewed annually or sooner if legislation, technology, or council needs change.

17. Contacts
For IT-related enquiries or assistance, users should contact the Parish Clerk

Adopted at the Parish Council meeting: 9 October 2025
Reviewed: 12 March 2026

Review Date: March 2027