Woodnewton Parish Council IT Policy

1. Purpose and Scope

This IT Policy is designed to protect council data, ensure compliance with UK GDPR, Data Protection Act 2018, and Assertion 10, and safeguard IT systems. It applies to all councillors, staff, and volunteers using council IT resources, including council-owned and personal devices used for council business.

2. Roles and Responsibilities

- Clerk / Responsible Officer: overall responsibility for IT systems and data security.
- Councillors and Staff: expected to follow the policy, report incidents, and maintain security.
- Training: council members and staff must complete training as directed.

3. Acceptable Use

Council IT systems and devices must be used appropriately for council business.
Prohibited activities include:

- Personal use for inappropriate content
- Unauthorized software installation
- Sharing passwords
- Using personal devices without security measures in place

4. Data Protection

- Comply with UK GDPR and Data Protection Act 2018.
- Collect, store, and share personal data lawfully, fairly, and transparently.
- Keep data only as long as necessary and dispose of securely.
- Respond to Subject Access Requests (SARs) as per procedures.
- Recognize council roles as Data Controller and Data Processor.

5. Cybersecurity

- Use strong passwords with regular changes.
- Ensure all devices and software are kept up to date.
- Install and maintain antivirus/anti-malware software.

- Secure networks and Wi-Fi; use encryption where needed.
- Regularly back up data and test recovery procedures.

6. Email and Communication

- Use council email addresses for official business.
- Do not share sensitive data via personal email.
- Be vigilant against phishing and suspicious links.

7. Remote Working

- Access council systems securely when working remotely.
- Ensure devices are protected and data is not stored insecurely.

8. Incident Reporting

- Report IT incidents promptly, including data breaches, malware infections, or lost/stolen devices.
- Follow council procedures for incident management.

9. Monitoring and Compliance

- IT systems may be monitored for misuse.
- Non-compliance may result in disciplinary action.
- Policy will be reviewed annually.

10. References and Supporting Documents

- UK GDPR guidance (ICO website)
- Data Protection Act 2018
- Council-specific data retention schedules and procedures
- Assertion 10 compliance guidance

Signed: _____ Date: _____