# Woodstock Town Council
## Information Technology Policy

### 1. Introduction

Woodstock Town Council ("the Council") recognises that the effective use of Information Technology (IT) resources, secure communication systems, and responsible data handling are essential to conducting its business transparently, efficiently, and securely. This policy outlines how IT and communication resources should be used by Councillors, staff and volunteers to comply with legal and regulatory standards and to protect the Council's data and systems.
This policy should be read in conjunction with the Council's Data Protection Policy, Code of Conduct, and Social Media Policy.

### 2. Scope

This policy applies to all individuals who access, use, or manage Woodstock Town Council's IT resources, including:

- Desktop computers, laptops, mobile phones, tablets
- Email accounts ending in *.gov.uk*
- Cloud-based services such as SharePoint, Microshade VSM Apps or Microsoft 365
- Internet access, printers, and networking hardware
- Digital storage, backups, and IT management systems

### 3. Acceptable Use of IT Resources

- Council IT resources are provided for official Council business.
- Limited personal use may be permitted, but must not:
    - Interfere with Council duties
    - Violate this or any related policy
    - Involve offensive, illegal, or inappropriate content
- Users must not use Council IT systems for:
    - Commercial gain
    - Political campaigning
    - Distributing discriminatory, defamatory, obscene, or harassing content

### 4. Data Protection and Confidentiality

All use of IT must comply with the UK GDPR and the Data Protection Act 2018. Users must:

- Protect personal and sensitive data
- Store documents only on Council-approved systems
- Not forward emails or data to private email addresses
- Ensure any portable data devices (USBs, external drives) are encrypted and authorised

### 5. Security and Device Management

- All Council devices must be secured with passwords or biometric authentication
- Anti-virus software and system updates must be kept current
- Only authorised software is to be installed; unauthorised installations are prohibited
- Personal devices must not be used to store Council data without prior approval

When working remotely:

- Ensure secure access (e.g. via VPN or authorised SharePoint login)
- Use password-protected files when sending confidential information



| | | | |
|---|---|---|---|
| **Date Adopted:** | | **Minute Number:** | |
| **Updated:** | | **Minute Number:** | |
| **Review Date:** | | **Minute Number:** | |

## 6. Email Usage

- All Councillors are issued with a Council email address (e.g. name@woodstock-tc.gov.uk) which **must be used for Council business**
- Email accounts:
    - Must not be forwarded to personal accounts
    - Should include a standardised signature and professional tone
    - Should be checked regularly
- Confidential information must only be shared with password-protected attachments
- Emails are legally considered records and should be retained where relevant

## 7. Internet and Social Media Use

- Internet usage must align with Council business needs
- Users must not:
    - Download pirated or unauthorised materials
    - Post defamatory or offensive content under the Council's name
- Councillors using **personal social media accounts** must ensure any statements are clearly personal and not representative of the Council unless officially authorised

## 8. Software Licensing and Intellectual Property

- The Council will comply with all software licensing terms
- Only the Council's IT support provider is authorised to install or configure software
- Copying, removing, or altering software without permission is prohibited

## 9. Monitoring and Oversight

The Council reserves the right to monitor IT usage to:

- Prevent inappropriate activity
- Detect data breaches or security incidents
- Ensure compliance with laws and Council policies
- Maintain service performance and integrity

Monitoring may include (but is not limited to):

- Email scanning
- Website access logs
- Device audits and file inspections
- Telephone call logs

Council will ensure that monitoring is proportionate and legally compliant, and data collected will be stored securely and only accessed when necessary.

## 10. Reporting Security Incidents

All users must immediately report:

- Lost/stolen devices
- Suspicious emails or cyber threats
- Unauthorised access attempts
- Data breaches or information loss

Reports should be made to the Clerk or designated IT contact (Microshade VSM Apps).

## 11. Responsibilities and Training

All users are responsible for:

- Keeping Council data secure
- Following this and related policies
- Using Council systems with integrity

Training and guidance materials will be provided or signposted periodically.

## 12. Breach of Policy

| | | | |
|---|---|---|---|
| **Date Adopted:** | | **Minute Number:** | |
| **Updated:** | | **Minute Number:** | |
| **Review Date:** | | **Minute Number:** | |

A breach of this policy may result in:

- Suspension of IT access
- Referral to the Monitoring Officer or Full Council
- Disciplinary or legal action if warranted

Any individual who believes this policy has been breached in relation to their personal information may raise the issue via the Council's **formal complaints or grievance procedure**.

## 13. End of Tenure or Role

When a Councillor or staff member leaves the Council:

- All Council devices and access credentials must be returned
- Email accounts and digital access will be disabled
- Any sensitive documents in their possession must be returned or deleted

## 14. Policy Review

This policy will be reviewed annually, or as needed in response to changes in legislation, technology, or best practice.

## 15. Contact and Support

For queries, support, or to report incidents, contact the Town Clerk.

Postal address: Town Hall, Market Place, Woodstock, OX20 SL
Email: clerk@woodstock-tc.gov.uk
Telephone: 01993 811216



| | | | |
|---|---|---|---|
| **Date Adopted:** | | **Minute Number:** | |
| **Updated:** | | **Minute Number:** | |
| **Review Date:** | | **Minute Number:** | |