# Shawbury Parish Council

## IT and Email Policy

To report security incidents or for help with IT, contact the Parish Clerk.

### 1. Introduction

Shawbury Parish Council understands how important it is to use email and IT safely and properly. This policy gives clear rules for how staff, councillors, and others should use council IT and email.

### 2. Scope

This policy applies to anyone using the Council's IT equipment or email, including computers, networks, software, devices, and accounts.

### 3. Responsibilities

All staff and councillors are responsible for the safety and security of Shawbury Parish Council's IT and email systems.

### 4. Acceptable use of IT resources and email

Council IT and email should mainly be used for council work. Small amounts of personal use are allowed if it doesn't affect work. Users must behave ethically and not access anything offensive or illegal.

### 5. Device and software usage

The Council provides a laptop, hard drive and software to the Clerk. Personal or unapproved software must not be installed on work devices.

### 6. Data management and security

Sensitive data will be kept safe and secure. Approved tools will be used for storing and sending data. Data will be backed up regularly and old data will be destroyed safely.

### 7. Network and internet usage

Internet use on Council devices must only be for council work. Copyrighted content must not be downloaded or shared without permission.

### 8. Email communication

The Council's email addresses must be used for council work only. Emails must be kept professional and respectful. Private information should only be sent in an encrypted form. Links and attachments from unknown sources must not be opened.

## 9. Password and account security

Passwords must be strong and must be kept private. They should be changed regularly to stay secure. Alternatively a password manager, such as KEEPER should be installed and used. Council email should use 2-step verification.

## 10. Mobile devices and remote Work

If mobile devices are provided, they must be protected with a passcode or fingerprint. IT safety rules apply to mobile devices and when remote working.

## 11. Email monitoring

The council may check emails to make sure this policy is being followed. This will be done legally and respectfully and only when required for a specific purpose.

## 12. Retention and archiving

In line with the Council's data retention policy, important emails must be kept, as required by law. Unnecessary emails will be deleted regularly.

## 13. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk or by the Clerk to the Chair of the Council.

## 14. Training and awareness

The council will provide training and/or advice to help staff and councillors stay safe when using IT and email.

## 15. Compliance and consequences

Not complying with this policy may result in losing IT access or other consequences.

## 16. Policy review

This policy will be reviewed annually. Between these reviews, updates may be made to address emerging technology trends and security measures.

| | |
|---|---|
| Reviewed | May 2026 |
| Review Frequency | Annually |
| Next Review due | May 2027 |