Upton Snodsbury Parish Council

IT Policy

Effective from April 1st, 2026

1. Introduction

Upton Snodsbury Parish Council, henceforth known as “the Council”, recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by councillors, employees, volunteers, and contractors, henceforth known as “Members”.

2. Scope

The Council provides and maintains IT resources — including software and email accounts — to facilitate the efficient discharge of council duties. This policy applies to all Members authorised to use these resources.

The Council acknowledges that Members may utilise personal devices to fulfil their official roles. However, adherence to these security protocols is **mandatory** regardless of device ownership. Compliance ensures the integrity of council data, protects against digital threats, and upholds public accountability.

3. Training and awareness

The Council will source training and resources to educate users about IT security best practices, privacy concerns, and technology updates as required/requested. Members should engage in training on email security and best practices, including but not limited to:

- the Parish Council Domain Helper Service’s virtual cybersecurity workshops for councils

- The National Cyber Security Centre Cyber Security training for small organisations and free Cyber Action Toolkit.

4. Acceptable use of council provided IT resources and email

When using IT resources for the Council’s purposes, Members must adhere to ethical standards, and respect copyright and intellectual property rights.
Where possible, authorised software, applications, websites and email addresses will be provided by the Council for work-related tasks.

Upton Snodsbury Parish Council

IT Policy

Effective from April 1st, 2026

Where the Council has provided a device, Members must not install unauthorised software without checking with the clerk, and must not use equipment or email to access or forward inappropriate or offensive content.

5. What Members must do if using their own personal devices

Where Members are using their own devices, they must make sure they are:

- using strong passwords for all their accounts (preferably using a password manager)
- downloading the latest operating system security updates
- using anti-virus software

6. Network and internet usage

Members must be careful about which Wi-Fi networks they join whist undertaking Council business. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. Members must always make sure they are using a trusted internet connection, which is password protected when carrying out official business.

7. Password and account security

Members are responsible for maintaining the security of their accounts and passwords. Use the National Cyber Security Centre's advice for choosing a strong password. For business continuity, login details and passwords need to be stored securely so they can be accessed by trusted individuals in an emergency.

8. Email communication

The Council will provide Members with an official email account for organisation-related communication only. Members must transition from using their personal email account to an official email account as soon as practically possible.

Members must make sure that emails are professional and respectful in tone.

When sending confidential or sensitive information, Members must ensure it is being sent to the correct and appropriate recipients.

Upton Snodsbury Parish Council

IT Policy

Effective from April 1st, 2026

Always be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify the source by looking at the email it has come from carefully. Do not download and open anything if unsure who has sent it.

9. Email access

The Council reserves the right to check email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. The Council clerk may need to access emails in responding to Freedom of Information (FOI) or subject-access requests. If using a personal email account for council business, this is still subject to data protections laws and FOI requests.

10. Data management, data retention and security

All sensitive and confidential data should be stored and transmitted securely. Members must regularly backup any important data to prevent data loss, regularly reviewing and deleting unnecessary emails to maintain an organised inbox.

11. Reporting security incidents

All suspected security breaches, including email breaches or incidents, should be reported immediately to the Council clerk.

12. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges.

13. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

14. Contacts

Upton Snodsbury Parish Council

IT Policy

Effective from April 1st, 2026

For IT-related enquiries or assistance, users can contact the Council Clerk or Council Members. Additional IT support is provided via the Parish Council Website provider, which will be coordinated via the Clerk or fellow Council Members as appropriate.

---

15. Approvals and Review

Date of adoption: 10/03/2026 at a meeting of the Upton Snodsbury Parish Council on 10 March 2026, Minute reference: 26/17
Date for next review: 10/03/2027