



IT Policy

1. Introduction

Upton parish council recognises the importance of effective and secure information technology (IT) and email usage in supporting its work and communications.

This policy sets out clear rules for how councillors, staff and contractors should use council IT systems, devices, and email accounts to protect data, comply with the law, and ensure smooth council operations.

2. Scope

This policy covers:

- Council **authorised devices** which are provided by Upton Parish Council and used by employee/(s). This includes computers, software, mobile devices, data, and email accounts.
- Councillors' **personal devices**, which are used by Upton Parish Councillors to host and access Upton Parish Council email accounts. Councillors are not provided with council authorised devices.

This policy does not cover:

- Network and internet connection as Upton Parish Council does not have a proprietary network or internet connection.
- Volunteers, as volunteers do not access Upton Parish Council IT resources.

3. Email

Authorised Devices

Upton Parish Council IT email accounts are to be used for official council-related communications, activities and tasks only.

All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

Emails should be professional and respectful in tone. As council emails may be subject to public disclosure under legitimate FOI requests, users should take care to ensure all correspondence remains appropriate and in keeping with council standards.

Users should be cautious with attachments and links, to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

Suspicious emails should not be forwarded, even to warn others not to open them, as this increases the risk of the recipient falling victim to a scam or cyber-attack.

Upton Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and UK GDPR.

Personal Devices

As above.

4. Software usage

Authorised Devices

Employees must use authorised software and applications provided by Upton Parish Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

Personal Devices

The policy cannot govern what software is installed on personal devices, as they are not owned or provided by Upton Parish Council.

5. Data management and security

Authorised devices

- The Clerk is the custodian of official Council data. It is stored securely in **Microsoft 365** on authorised devices providing ongoing cloud backups and version history to support data recovery.
- Employee/(s) must follow the Council's **Data Protection Policy** and UK GDPR principles (lawfulness, fairness and transparency; purpose limitation; minimisation; accuracy; storage limitation; security; integrity and confidentiality).
- Personal data will be retained only for as long as necessary to fulfil the purposes for which it was collected. The Council will regularly review data retention periods to ensure compliance with legal requirements.
- Employee/(s) will redact personal data before forwarding to Councillors unless consent or other lawful purpose has been obtained.

Personal devices

- Councillors **must** follow the Council's **Data Protection Policy** and UK GDPR principles (lawfulness, fairness and transparency; purpose limitation; minimisation; accuracy; storage limitation; security; integrity and confidentiality) irrespective of whether they are using a personal device.
- Council data should not be stored permanently on personal devices unless it is in the public domain.
- Council data should be permanently deleted from personal devices once it is no longer required for the purpose it was collected/acquired.

Confidential and sensitive data

- Upton Parish Council is committed to the principles of openness and transparency, except where restricted by applicable legislation.
- Instances of sensitive and/or confidential data are few and will usually be dealt by the Clerk, using authorised devices and software.
- In a limited number of legitimate circumstances, Councillors need to deal with confidential and/or sensitive data. These may include, but are not limited to:
 - Accessing electoral roll for completion of nomination forms
 - Recruitment of staff
 - Staff grievances, sickness and absence, disciplinary matters
 - Dealing with a complaint
 - Some legal proceedings
- Councillors choosing to request a copy of the electoral roll or volunteering for Staffing Committee, Complaints Committee, Grievance Committee and other tasks involving sensitive and/or confidential data, should provide assurances to Upton Parish Council that their personal devices are secure and adequately protected.
- Encryption may be required for sending confidential data by email.
- Data must be permanently deleted from personal devices once it is no longer required for the purpose for which it was collected/acquired.

7. Other forms of digital communication

Upton Parish Council does not use WhatsApp/Messenger or any other direct messaging applications to conduct official council business.

8. Password and account security

Authorised Devices

Upton Parish Council employee/(s) are responsible for maintaining the security of their accounts and passwords.

Passwords should be strong and not shared with others.

Multi-factor authentication should be enabled where applicable.

Passwords should be changed immediately if you suspect it has been compromised.

Secure all mobile devices with passcodes, PINs, or biometric authentication.

Lock screen when not in use.

When working remotely, follow the same security practices as in the office.

Personal Devices

Upton Parish Councillors should aim for the same level of password and account security as employees, but this policy cannot govern what security is used on personal devices, as they are not owned or provided by Upton Parish Council.

Councillors unable to provide this level of password and account security on their personal devices should inform the Clerk. They should avoid volunteering for committees or tasks involving use of confidential/sensitive data (see section 5) and should contact the Clerk for specific electoral roll numbers, in lieu of requesting a copy of the full register.

9. Reporting security incidents

Report all suspected IT security incidents immediately to the Clerk and the IT provider. Examples include:

- Clicking a suspicious link or opening a suspect attachment
- Loss or theft of a device containing council data
- Suspected hacking or unauthorised access.

The Clerk will report data breaches in accordance with Data Breach Policy.

Initial response target: **within 24 hours**. Notify the Information Commissioner's Office (ICO) within 72 hours.

All incidents will be recorded and investigated, with findings reported to the council and/or the ICO as determined by the nature of the breach.

10. Training and review cycles

Councillors and staff will receive annual refresher training on data protection and cyber security.

Adopted: March 2026

Review: