

Walsham le Willows Parish Council IT Policy

Adopted at meeting of Council on 13/05/2026

1. Introduction

Walsham le Willows parish 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 council members, employees, volunteers, and contractors.

2. Scope

This policy applies to all individuals who use of any Walsham le Willows parish council IT resources, if provided, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Any Walsham le Willows parish council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

Where possible, and proportionate, authorised devices may be provided. Walsham le Willows parish council doesn't currently provide any authorised devices. Software and applications provided by 3rd parties for installation on personal devices should be used only for work-related tasks.

Unauthorised installation of software on any provided authorised devices, including personal software, is strictly prohibited due to potential security issues.

5. Data management and security

All sensitive and confidential Walsham le Willows parish council data is now stored in applications and on cloud platforms provided by 3rd party suppliers and is thus stored and transmitted securely using approved methods. Regular data backups are

provided by the 3rd party suppliers to guard against data loss, and which ensure secure data destruction methods when necessary.

6. Network and internet usage

Walsham le Willows parish council does not provide dedicated network and internet connections. If these were to be provided they must be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

.gov.uk email accounts provided by a 3rd party for Walsham le Willows parish council are for official communications only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

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

8. Password and account security

Walsham le Willows parish council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others or written down.

It is suggested to councillors that they should create a strong password for their personal devices of at least 8 characters which includes upper and lower case letters, numbers and symbols, otherwise use 2Factor or biometric authentication which is increasingly ubiquitous.

It is suggested that they create a distinct password that can be used for applications accessing Council email accounts or cloud storage.

An alternative is a passphrase made up of 4-5 words that are memorable to them, and preferably random. The strength of these can be reliably and safely tested here: <https://www.grc.com/haystack.htm>

9. Mobile devices and remote Work

Mobile devices are not currently provided by Walsham le Willows parish council, but if any were to be supplied, they should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same

security practices as if they were working in an office. Walsham le Willows Parish Council currently has no office premises.

10. Email monitoring

Walsham le Willows 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 GDPR.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Emails should be regularly reviewed and deleted to eliminate unnecessary emails and to maintain an organised inbox.

Any parish council documents that are stored should be stored within the cloud storage areas as demonstrated and facilitated by the Clerk. Each councillor has 5GB of free storage. Most will be read, and should remain, on the shared storage as made available by the Clerk.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact (Parish Clerk) for investigation and resolution. Report any email-related security incidents or breaches to the the Clerk immediately.

13 Training and awareness

Walsham le Willows parish council may provide, at its discretion, training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors are asked to read the appendix below on best practices and awareness.

14. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of accounts and access to parish council email and shared areas.

15. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness.

16. Contacts

For IT-related enquiries or assistance, users can contact the Parish Clerk.

All staff and councillors are responsible for the safety and security of Walsham le Willows parish council's IT and email systems. By adhering to this IT and Email Policy, Walsham le Willows parish council aims to create a secure and efficient IT environment that supports its mission and goals.

APPENDIX

Information tailored from : <https://emailanalytics.com/21-email-security-best-practices-every-professional-must-know/>

Key Terms

- Phishing: A scam where attackers mimic trusted authorities (banks, websites) via email to trick recipients into revealing passwords, credit card numbers, or other personal information.
- Two-factor authentication (2FA): A security method requiring two pieces of identifying information to log in—typically a password plus a temporary code sent to your mobile device.
- End-to-end encryption: A security protocol where only the sender and recipient can read email contents, preventing interception by third parties including email providers. [To all intents and purposes impractical in the real world as things stand. KB]
- Malware: Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems, often spread through email attachments.

Email security isn't something to be taken lightly. For many organizations, email is the most important communication channel. If someone gains access to your account, it could open the door to data breaches.

Most would-be hackers and competitors are opportunists looking for low-hanging fruit like simple and obvious passwords. Even routine, basic security

practices will protect you from the vast majority of threats. Here are 21 email security best practices every professional must know.

How Do You Create and Manage Secure Email Passwords?

Short answer: Use strong, unique passwords for each account with a mix of characters, change them regularly, never share them, and enable two-factor authentication.

1. Use a Strong Email Password

With [2 million people using “123456” as a password](#), this topic is worth exploring. Most cybercriminals don’t brute-force their way into accounts—they guess passwords or use social engineering. A “strong” password is hard to guess.

Make your password stronger by using a mix of lower-case letters, upper-case letters, numbers, and special symbols. Make it longer—each character multiplies possible combinations. Avoid easy-to-guess combinations like your company name, birthday, or simple sequences like “1234.”

2. Use Different Passwords for Different Accounts

Once you create a strong password, you’ll be tempted to use it everywhere. Don’t. If a hacker gets your password for one account, they’ll try it with others connected to your name. Use unique passwords for each account so one breach doesn’t compromise everything. Use a password manager secured with one strong password you have to remember to store your passwords. [KeePass is a free example for Windows](#).

3. Change Your Password Regularly

Change your passwords at least once a year. After data breaches, thieves sometimes sit on stolen data for weeks to years until attention dies down. Regular password changes prevent these time-delayed attacks and make your password harder to guess since it’s never the same for too long.

4. Never Give Out Your Password

No reputable email company will ever ask for your password directly, over email or phone. If someone claims to be from Gmail and asks for your password, it’s almost certainly a scam. Don’t even discuss your password with friends or write it on a sticky note. Keep it private at all times.

5. Enable Two-Factor Authentication

Increasingly websites offer two-factor authentication (also called 2-step or multi-factor authentication). This prompts you for two pieces of identifying information—usually a password plus a temporary code sent to your phone. While slightly inconvenient, it only takes seconds and provides an extra barrier of protection if your password is compromised.

6. Methods of for securing email

More and more of these strategies will become available . For example Gmail has a built-in “Confidential” mode for sending emails more securely. Open the Compose window, click the lock-and-clock icon in the bottom row. Once enabled, recipients cannot forward, copy, print, or download the message contents. This helps [prevent confidential information from spreading](#) beyond intended recipients.

You can set an expiration date so the message self-destructs, and require the email to be unlocked with a unique SMS passcode sent to your recipient’s mobile device—preventing the message from being seen by prying eyes.

NB Clerk: However nothing is foolproof. Gmail's Confidential Mode does not prevent . recipients from capturing content using screenshots or other methods, despite the restrictions on forwarding, copying, or downloading. Email message expiration and unlock codes have not been generally adopted probably because of the perceived inconvenience.

7. Consider Encryption Add-ons if they are available for your email provider

Gmail is friendly to third-party developers, and there are hundreds of [Gmail apps, add-ons, and extensions](#) to improve your email experience. Some focus specifically on security—for example, [FlowCrypt](#) or [Virtru](#) can secure your attachments and messages with end-to-end encryption.

How Should You Manage Your Email Accounts Securely?

Short answer: Keep personal and work accounts separate, log out when finished, avoid giving away your email address unnecessarily, and regularly review security settings.

8. Don’t Mix Personal and Professional Email Accounts

Avoid using your personal account for professional emails or vice versa. If you use your work email for personal communications, it opens the door to more

security risks. If you exchange work-related information on a private account, it becomes vulnerable if that personal account is ever hacked. Keep accounts segmented. It's all about layers of security.

9. Avoid Giving Your Email Address Away

Resist giving your email address to every website that requests it. While most businesses only use it for newsletters, some sell your information to third parties or make it public, exposing you to more email threats. If you don't have to give it out, don't. Or use a different address/alias for unimportant registrations.

10. Log Out When Finished

Log out of your email account. This is especially important on unfamiliar devices or networks, but should be adopted 100% of the time. It makes it harder for someone to access your email just by starting your device.

11. Periodically Review Security Settings

How Do You Recognize and Avoid Email Scams?

Short answer: Learn common scam types (phishing, Nigerian Prince), verify suspicious senders through other channels, investigate unusual URLs (the web addresses that appear in the address bar of your browser), and never provide personal information via email.

12. Be Aware of Email Schemes

Many scammers use email because it's cheap and infinitely scalable. You can guard against most scams simply by knowing they exist.

Phishing is one of the most common schemes, where emails mimic trusted authorities (your bank, eBay) to trick you into revealing personal details. Also watch for Nigerian Prince scams, guaranteed loans, lottery winnings, disaster relief scams, and shady offers on items you're buying or selling online.

13. Investigate Suspicious Messages

If a message seems even slightly suspicious, investigate it. Search online for the subject line or message contents—you'll often find pages identifying it as a scam. You probably aren't the first target. If the message appears to come from a trusted source, contact them through another channel to verify.

14. Investigate Suspicious URLs

Before clicking any link, especially from unfamiliar or unexpected sources, investigate. Scammers may replace one letter in a domain name (part of the web address) to fool you—like paypal.net instead of paypal.com, or goggle.com instead of google.com. They may also use link shortening services to disguise malicious URLs. Most shortening services (like TinyURL) let you preview links before clicking.

15. Never Give Away Personal Information in Email

No reputable company will ask for personally identifying information over email. If anyone asks for your birthday, social security number, credit card number, or password, it's almost certainly a scam. Contact the company directly using information you find online (not from the suspicious email) to verify the request.

16. Avoid Replying to Scammers

If you've identified a scammer, don't reply—even to give them a piece of your mind. Responding verifies that your email address is valid, opening the door to more attacks. The response may not even reach the intended recipient anyway.

How Do Device and Network Choices Affect Email Security?

Short answer: Only access email on secure devices, avoid public Wi-Fi, and keep antivirus software installed on all devices you use for email.

17. Be Careful Which Devices You Use

Many companies now have bring-your-own-device (BYOD) policies, but this can be dangerous. If your personal device is infected with malware, logging into your professional email could expose you to hacking. Take security precautions with every device you use for email.

18. Be Careful Which Wi-Fi Networks You Use

Only access email when you're confident in your network's security. Publicly accessible and unsecured Wi-Fi is risky—anyone on the network could hypothetically monitor your actions and access personal information. Stick to trusted Wi-Fi networks.

19. Keep Antivirus Software Installed

Keep antivirus software installed on your machine. Most antivirus programs automatically scan email attachments before download and prevent access to malicious webpages. They can also remove malware that makes its way onto your computer. [Norton](#) is the biggest name, but [AVG](#) is a free option that does most of the same things. [MalwareBytes](#) is another big and trusted name.

How Do You Handle Email Attachments Safely?

Short answer: Never open attachments from untrusted sources. Verify unexpected attachments by contacting the sender through another channel before opening.

20. Never Open Untrusted Attachments

Attachments are the most common way to spread malware. Opening an attachment downloads it to your computer, potentially including malicious scripts or programs. Many attempts use strange or zipped file types, but some arrive disguised as conventional files like .jpg or .pdf.

Only open attachments that match your expectations from users you trust. If you're ever in doubt, call the sender and ask them to verify the contents before opening.