

Shouldham Parish Council IT Policy

Adopted 04 March 2026

Reviewed

1. Introduction

Shouldham 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 Shouldham Parish Council's or personal IT resources, including computers, tablets, 'smart' phones networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Shouldham Parish Council IT resources and all Council 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, authorised devices, software, and applications will be provided by Shouldham Parish Council for work-related tasks.

Councillors are expected to use their own devices for conducting Council business. However, it is accepted in line with [ICO guidance fact sheet](#) that there are inherent risks with using your own devices and Councillors should consider the following key points and mitigate accordingly:

- Who else can access the Cllr email account or privately-owned device?
- How can you control and maintain separation of Council and personal data and email accounts on privately owned device (eg accuracy and retention)?
- How much consideration has been given to the data on the device being overlooked?
- How secure are the devices (eg is the device password-protected and what is the risk of malware)?
- What if the device is lost or stolen – can you remotely locate it and wipe the data?
- What operating system is the privately-owned device running?
- How is data transferred to other devices, and how secure are these systems and/or devices?

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

5. Data management and security

All sensitive and confidential Shouldham Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

6. Network and internet usage

Shouldham Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Shouldham Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted. Stackmail, the platform for the Council's .Gov accounts, uses SSL/TLS encryption, protecting it whilst in transit between your email account and the server and then between server and your email account.

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

Shouldham Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Passwords reminders should be stored in a secure manner. Regular password changes are encouraged to enhance security.

9. Mobile devices and remote work

Mobile devices provided by Shouldham Parish Council should be secured with passcodes and dual factor authentication where possible. When working remotely, users should follow the same security practices as if they were in the office.

10. Email monitoring

Shouldham Parish Council reserves the right to monitor official email communications to ensure compliance with this policy and relevant laws. Monitoring may be conducted in accordance with the Data Protection Act and GDPR and it should be noted that the ICO has the powers to review personal email and IT devices that are used to conduct PC business.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk in the first instance for investigation and resolution. Report any email-related security incidents or breaches to the provider (Norfolk ALC IT Officer) via the Clerk immediately.

13 Training and awareness

Shouldham Parish Council will provide regular training and resources to educate users about GDPR and IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

14. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT and digital communication privileges and further consequences as deemed appropriate.

15. 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.

16. Contacts

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

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