Shireoaks Parish Council - IT Policy

Adopted Date: 14th April 2026

Review Date: April 2028

1. Introduction

Shireoaks Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy provides a framework for the effective, secure and responsible use of information technology within Shireoaks Parish Council

The policy ensures that the council:

• protects its information and IT systems
• manages digital communication responsibly
• complies with relevant legislation including the UK General Data Protection Regulation and the Data Protection Act 2018
• follows best practice guidance issued by the National Association of Local Councils
The Clerk to the Council is responsible for the day-to-day administration of council IT systems.

2. Scope

This policy applies to

• all councilors, employees, and volunteers
• any device used to access council information or systems
• council email accounts, website systems and official social media platforms
This includes both council-owned devices and personal devices used for council business.

3. Acceptable use of IT resources and email

Council IT resources and email accounts are to be used for official council-related activities and tasks. All users must adhere to ethical standards as follows:

• act professionally when using council systems
• not access, download or distribute illegal, offensive or inappropriate material
• keep login details confidential
• log out of systems and lock devices when not in use

4. Council Email and Digital Communications

Council business should be conducted using official council email accounts where possible.

Councillors and officers should:

• use council email addresses for official communications where available
• avoid using personal email accounts for council business where possible
• ensure communications are professional and appropriate
• comply with the council's Code of Conduct
Care must be taken when sending confidential or personal information.

Sensitive information should only be shared where necessary and using secure methods where appropriate.

5. Device and software usage

Where possible, authorised devices, software, and applications will be provided by Shireoaks Parish Council for work-related tasks.

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

6. Data Protection and Information Security

Shireoaks Parish Council is committed to protecting personal data and handling information responsibly.

All users must:

• only collect or process personal data where necessary for council business
• ensure personal data is stored securely
• avoid unnecessary sharing of personal information
• follow the council's privacy notices and data protection procedures
Any suspected data breach or loss of personal data must be reported immediately to the Clerk.

7. Data management and security

All sensitive and confidential Shireoaks Parish Council data should be stored and transmitted securely using approved methods.

Up-to-date operating systems and software should be maintained.

Secure data destruction methods should be used when necessary.

Regular backups should be made of Important Council Documents:

• be stored securely
• allow information to be recovered in the event of data loss, cyber incident or hardware failure

8. Network and internet usage

Shireoaks 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.

Users should avoid accessing council systems through unsecured public Wi-Fi networks where possible.

9. Email communication

Email accounts provided by Shireoaks Parish Council are for official communication only. Emails should be professional and respectful in tone.

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

10.Cyber Security Awareness

Users should remain alert to cyber security risks including:

• phishing emails
• suspicious attachments or links
• fraudulent communications
Any suspicious activity or cyber incident should be reported to the Clerk immediately.

11. Password and account security

Shireoaks Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

12. Mobile devices and remote Work

Mobile devices provided by Shireoaks Parish Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

13. Email monitoring

Shireoaks 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.

14. Website and Social Media

Only authorised individuals may update the council website or post on official council social media accounts.

Content must:

• be accurate and appropriate
• reflect the council's role and responsibilities
• comply with legal and data protection requirements
Personal views must not be presented as the official position of the council.

15. Retention and archiving

Council files may be stored electronically using approved storage systems. Users should:

• only store council information on authorised systems
• avoid storing council files on personal accounts where possible
• ensure documents containing personal data are appropriately protected

16. Reporting security incidents

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

17. Compliance and consequences

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

18. Policy review

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

19. Contacts

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

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