Sibford Gower Parish Council
IT Policy

1. Introduction

Sibford Gower 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, Clerk, volunteers, and contractors.

2. Scope

This policy applies to all individuals who use Sibford Gower Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Sibford Gower Parish Council's 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. Data management and security

All sensitive and confidential Sibford Gower 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.

5. Network and internet usage

Sibford Gower 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.

6. Email communication

Email accounts provided by Sibford Gower 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. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

7. Password and account security

DRAFT

Sibford Gower 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.

8. **Mobile devices and remote work**

Mobile devices provided by Sibford Gower 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.

9**. Email monitoring**

Sibford Gower 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.

10**. 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.

11. **Reporting security incidents**

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately.

12. **Training and awareness**

Sibford Gower Parish Council will provide training and resources to educate users about IT security best practices, privacy concerns, and technology updates.

13. **Compliance and consequences**

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

14. **Policy review**

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

16. **IT-related enquiries or assistance**

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

DRAFT