Waldringfield Parish Council

IT Policy

Draft until adopted

Waldringfield Parish Council

IT Policy

1. Introduction

1.1. Waldringfield parish council (WPC) recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

1.2. This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

1.3. This policy defines how WPC manages its use of IT in line with the Transparency Code for Smaller Authorities (2015) and the 2025 edition of the Practitioners' Guide. It ensures the Council's digital operations are transparent, secure, and compliant with data protection laws.

2. Scope

2.1. This policy applies to all individuals who use WPC's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

3.1. WPC 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.

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

4. Governance and oversight

4.1. The Clerk is the designated Data Protection Officer (DPO) and IT systems operator. All Councillors oversee implementation, security and compliance.

5. Device and software usage

5.1. Where possible, authorised devices, software, and applications will be provided by WPC for work-related tasks.

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

6. Data management and security

6.1. All processing of personal data will comply with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

- **Privacy Policy:** All data collection, processing, and subject rights are governed by the WPC's Privacy Statement, available on the WPC website. All users will familiarise themselves with this.

- **Access and Storage:** Data is stored securely, with access granted only to authorized personnel based on necessity.

- **Retention:** Personal data will be retained in accordance with the WPC Data Protection Statement and securely deleted when no longer needed.

6.2. All sensitive and confidential WPC 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.

7. Network and internet usage

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

8. Email communication

8.1. Email accounts provided by WPC 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.

8.2. WPC is cautious with attachments and links to avoid phishing and malware. WPC will verify the source before opening any attachments or clicking on links.

9. Password and account security

9.1. WPC 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.

10. Mobile devices and remote Work

10.1. While currently not provided, mobile devices provided by WPC at any point in the future should be secured with passcodes and/or biometric authentication.

10.2. When working remotely, users should follow the same security practices as if they were in the office.

11. Email monitoring

11.1. WPC 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 2018 and GDPR.

12. Retention and archiving

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

13. Reporting security incidents

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

14. Training and awareness

14.1. WPC will make available regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will be provided with regular training on email security and best practices.

15. Compliance and consequences

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

16. Policy review

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

17. Contacts

17.1. For IT-related enquiries or assistance, users can contact the Parish Clerk at clerk@waldringfieldparishcouncil.gov.uk.

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