FIRSDOWN PARISH COUNCIL
Mrs AC Purves FSLCC, Parish Council Clerk
"Cranbourne", White Way, Pitton, Salisbury, Wilts, SP5 1DT
Tel: 07598 054675
https://www.firsdown-pc.gov.uk
e-mail: clerk@firsdown-pc.gov.uk

Firsdown Parish Council IT Policy

1. Introduction

Firsdown 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.

The following documents should also be read in conjunction with this policy:

- FPC GDPR Document retention and disposal policy
- FPC Cyber Security Policy

2. Scope

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

3. Acceptable use of IT resources and email

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

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

The following devices are authorised for carrying out the business of Firsdown Parish Council, and are under the custodianship of the Clerk:

- HP Pavilion Laptop 15-eg2019na, serial number 5CD2455841
- Samsung A3 2017 model phone number 07598 054675

5. Data management and security

All sensitive and confidential Firsdown 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

Firsdown Parish Council does not operate any network or server hardware. Only secure internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

The name@firsdown-pc.gov.uk email accounts provided by Firsdown 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.

8. Password and account security

Firsdown 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. Two factor Authorisation (2FA) should be used as an additional level of security where possible.

Passwords must not be kept with the IT devices, and the use of a Password manager application is recommended.

9. Mobile devices and remote working

Mobile devices provided by Firsdown Parish Council should be secured with passcodes and/or biometric authentication. When working remotely, (eg using the IT at a conference), users should follow the same security practices as if they were in the office.

10. Email monitoring

Firsdown 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 the Document Retention & Disposal Policy. 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 designated IT point of contact (Firsdown Parish Council Chairman) for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately (BWP Creative Ltd t/as Parish Council Website).

13 Training and awareness

Firsdown Parish Council will provide regular training and resources to educate users about 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 privileges and further consequences as deemed appropriate.

15. 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. Contacts

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

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

Date: _____

Signature: _____

Role: _____

Adopted: October 2025

Amended: November 2025

Review date: May 2026