

HERMITAGE PARISH COUNCIL IT POLICY

1. Introduction

Hermitage Parish Council (HPC) 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 Hermitage Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Device and software usage

Where appropriate, authorised devices, software, and applications will be provided by Hermitage Parish Council for work-related tasks. Installation of unauthorised software on HPC devices, including personal software, is strictly prohibited.

Current practice is that the Clerk shall be supplied with a laptop and mobile phone. These may be passed to councillors or other persons only when authorised by council, for example when the Clerk is absent.

HPC IT resources and email accounts are intended 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. Sensitive information

Sensitive and confidential Hermitage Parish Council data must not be transmitted by email unless it is encrypted or password protected. If there is a need to share sensitive information, it may be done by shared access to files on the cloud storage area.

5. Data back-ups and destruction

The Clerk shall hold all formal records on the HPC-supplied laptop and backed up to the cloud.

A copy shall also be made to a password-protected hard drive. This shall be passed to the Chairman for storage in a second location and exchanged for a second back-up drive at each council meeting.

Any council-supplied equipment and storage media shall be destroyed in a secure manner when no longer required.

6. Email communication

Email accounts provided by Hermitage 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.

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

Personal email accounts must not be used to send correspondence on behalf of HPC except in exceptional circumstances, e.g. loss of HPC service. [This restriction only applies to items other than contracts once gov.uk email accounts have been set up]

7. Password and account security

Hermitage 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 also encouraged to enhance security.

8. Device and Data Security

All devices and accounts provided by Hermitage Parish Council should be secured with passcodes and/or biometric authentication.

A note shall be made of all logins and passcodes for council-supplied equipment and shall be handed to and retained by the Chairman or Clerk in a sealed dated envelope for storage at a second location. This envelope may not be opened other than in the presence of two other councillors. After the envelope has been opened, in any circumstances, the passcodes shall be changed as soon as practicable. The fact that the sealed envelope has been opened, in whatever circumstances, shall be reported to all councillors immediately and formally to the next available council meeting.

No employee or councillor shall disclose any PIN or passcode relevant to the working of the council or its bank accounts to any person not authorised in writing by the council.

The council, and any members using computers for the council's financial business, shall ensure that anti-virus, anti-spyware and firewall software is used with automatic updates. Use of a VPN is recommended.

Access to any internet banking accounts must be directly to the access page (which may be saved under 'favourites') and not through an email link or other web page. Banking work, other than payment authorisation, may only be carried out on the council owned computer.

9. Email monitoring

Hermitage 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. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution.

11. Leaving office

On leaving office, Councillors and employees shall return any HPC property and delete any council-related emails, files, log-in details etc from personal computers and accounts within 7 days.

The Clerk shall arrange to cancel any accounts and permissions assigned to the individual as soon as practicable.

12. Training and awareness

All staff and councillors should undertake appropriate training in relation to IT security best practices, privacy concerns, and technology updates.

13. Compliance and consequences

Breach of this IT Policy may result in the suspension of IT privileges and further consequences as deemed appropriate according to the seriousness of the offence.