Peasenhall Parish Council IT Policy

1. Introduction

Peasenhall 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.

2. Scope

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

3. Acceptable use of IT resources and email

Peasenhall 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, devices, software, and applications will be provided by Peasenhall parish council for work-related tasks.

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

5. Bring Your Own Device (BYOD)

Users may use their own devices for accessing Council resources, e.g. Email. Where sensitive data is being handled, it must not be stored on the device, and the device must be protected by the Council's approved end point security (ESET).

6. Data management and security

All sensitive and confidential Peasenhall 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/device disposal methods should be used when necessary. Guidance on secure data and device disposal can be obtained from the National Cyber Security Centre. Devices should be disposed of in accordance to Waste Electrical and Electronic Equipment (WEEE) guidelines or by using a WEEE accredited provider.

7. Network and internet usage

Peasenhall 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.

8. Email communication

Email accounts provided by Peasenhall 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. Council email is not encrypted. Only attachments that are encrypted using AES-256 or better should be used to send sensitive or confidential data. Passwords for decryption must be sent separately either by text or telephone.

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

9. Password and account security

Peasenhall 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. Passwords must not be shared between accounts.

The following is a guide for strong passwords

- Length is Priority: Use at least 15-16 characters; longer is always better.
- Randomness: Avoid dictionary words, personal information (birthdays, names, pet names), or common patterns like "123456" or "password".
- Use a mixture of upper and lower case characters, numbers and special characters.
- Unique for Every Account: Never reuse passwords, as a breach on one site can compromise others.

- Use a Passphrase: Combine 3–4 random, unrelated words to create a long, memorable string.

10. Mobile devices and remote Work

Mobile devices provided by Peasenhall 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. Users must not connect their devices to unsecured (open) WiFi networks.

11. Email monitoring

Peasenhall 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.

12. 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.

13. 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 Parish Clerk immediately.

14. Training and awareness

Peasenhall 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.

15. Compliance and consequences

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

16. Policy review

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

For IT-related enquiries or assistance, users can contact Peasenhall Parish Council clerk.

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

Date: _____

Signature: _____

Role: _____

Document Version : 2026-03-27-002