

Barningham Parish Council IT policy

1. Introduction

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

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

2. Scope

This policy applies to all individuals who use Barningham parish council's IT resources, including computers, networks, software, devices, and data. Resources include access to .gov.uk email addresses, any associated digital storage and social media.

3. Acceptable use of IT resources

Barningham parish council IT resources, where provided, are to be used for official council-related activities and tasks. Personal use should not interfere with Barningham parish council work responsibilities.

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 the Barningham parish council for work-related tasks. Installation of software on authorised devices, including personal software, is at the Clerks discretion.

5. Data management and security

All sensitive and confidential Barningham 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

Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Barningham parish council are for official communication only. Email signatures should be used and emails should be professional and respectful in tone. Emails containing sensitive/confidential information should be password protected where possible.

Be cautious when opening email attachments or clicking on links to prevent phishing and malware threats.

8. Password and account security

Barningham 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.

9. Mobile devices and remote work

Mobile devices provided by Barningham parish council should be secured with passcodes and/or biometric authentication.

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. Training and awareness

Barningham parish council will provide regular access to resources to educate users about IT security best practices, privacy concerns, and technology updates.

12. Compliance and consequences

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

13. 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.

14. Contacts

For council IT-related enquiries or assistance, users can contact in the first instance, the Clerk.

All staff and councillors are responsible for the safety and security of Barningham Parish Council's IT resources. By adhering to this IT policy, Barningham Parish Council aims to create a secure and efficient IT environment that supports its functions.