IT Policy

Introduction

1. Headbourne Worthy Parish Council recognises the importance of effective and secure information technology (IT), data security, and email usage in supporting its business, operations, and communications.

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

Scope

3. The policy applies to all individuals who use Headbourne Worthy Parish Council's IT resources, including computers, software, data, and email accounts.

Council IT Resources

4. The Parish Council laptops and storage devices are for official council related activities and tasks and should only be used by authorised staff. In exceptional circumstances, the Clerk may authorise the use of council IT equipment by councillors.

5. The Clerk is responsible for authorising the installation of software on Council owned IT equipment.

6. Council Staff must:

- Use strong passwords and not share them with others.
- Enable automatic screen locking
- Log out at the end of each working day
- Store devices securely when not in use

7. Regular password changes are encouraged to enhance security in accordance with the council's data protection

8. Limited personal use of equipment by council staff is permitted, provided it does not interfere with work responsibilities or violate any part of this policy.

9. All users must respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

10. Family members, volunteers or third parties must not use Council equipment.

11. Council data should be saved to the cloud. Any data saved on the hard drive of the Council's computer should also be backed up to the cloud.

12. Council-owned devices must have up-to-date antivirus software and receive regular software updates.

13. USB drives and external storage must be scanned before use.

Data Protection and GDPR

14. The Parish Council processes personal data lawfully, fairly, and securely.

15. The guidelines set out in the council's Data Protection Policy must be followed by everyone processing personal data.

16. All staff and councillors must:

- Only access data necessary for their role.
- Not share personal data without proper authority.
- Use official council email accounts.
- Delete or securely dispose of council data when no longer required
- Regularly review and delete unnecessary emails.

17. Any suspected security breaches or incidents must be reported **immediately** to the Clerk for investigation and resolution.

18. Emails and documentation should be retained and archived in accordance with the council's document retention policy and in accordance with any legal and regulatory requirements.

19. All sensitive and confidential council data should be stored and transmitted securely using approved methods.

20. Regular data backups should be performed to prevent data loss, and secure data.

Email Communication

21. Email accounts provided by Headbourne Worthy Parish Council are for official communications only and should always reflect the Parish Council decisions and policies. Emails should be professional and respectful in tone.

22. Confidential or sensitive information should not be sent via email unless it is encrypted.

23. Private email accounts must not be used for council business.

24. Mail sent to private email addresses regarding council matters must be re-directed to official council email address.

25. Emails that are no longer relevant must be deleted.

26. Attachments or links should not be clicked onto before the source is verified.

27. Headbourne Worthy Parish Council reserves the right to monitor email communications to ensure compliance with this policy, relevant laws and code of conduct. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

28. All Council emails are subject to Freedom of Information requests.

Use of Personal Devices

28. Councillors use their own devices (e.g. laptops, tablets, phones) for Council business, and staff may also use their own personal devices for limited Council business.

29. Anyone using personal devices must:

- Take reasonable steps to protect Council information
- Ensure confidential Council data cannot be accessed by others
- Follow GDPR requirements when handling personal data

30. The Parish Council does not monitor or manage the use of personal devices, but expects anyone using personal devices to apply appropriate security controls (see below).

Security Guidance for using Personal Devices

31. To prevent confidential Council information on personal devices being inadvertently accessed by family members or third parties, councillors and officers are strongly advised to:

- Use strong passwords, PINs, or biometric security
- Enable automatic screen locking
- Use separate user accounts if devices are shared with family members
- Ensure devices are encrypted where possible
- Avoid accessing confidential Council data on public Wi-Fi
- Take care when working at home that screens and papers cannot be seen by others.
- Log out of council email accounts after use
- Avoid saving Council documents to shared folders
- Securely delete Council files when no longer required
- Ensure old devices are wiped before disposal or resale

Compliance and Training

32. All members of staff and councillors are responsible for the safety and security of Headbourne Worthy Parish Council IT and email systems. By adhering to this IT policy Headbourne Worthy Parish Council aims to create a secure and efficient IT environment.

33. All employees and councillors will receive regular training on email security and best practices as required.

34. Any breaches of this IT policy will be investigated and may result in the Council's disciplinary process being enacted.