Mayfield and Five Ashes Parish Council

Information Technology Policy

Contents

1. Introduction
2. General Principles
3. Training and Guidance
4. IT Provision and Policy
   • Parish Clerk
   • Members
5. Data Management and Security
6. Websites and Social Media
7. Password Protection
8. Portable Devices
9. Incident Reporting
10. Misuse of IT
11. Risk Management

1 Introduction

Mayfield and Five Ashes Parish Council recognises the importance of effective and secure information technology (IT) hardware and software 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 and duty to ensure the proper security and privacy of its computer systems and data. All users are responsible for protecting these assets. It runs in conjunction with the Parish Council's Email and Internet Policy and its Social media Policy.

The Parish Clerk is responsible for implementing and monitoring this policy.

2 Definitions

Users: Councillors, employees and third parties acting on behalf of the Council.

Data: Digitally stored information including (but not limited to) documents, copyrighted / Copyrightable text, images, personal information, accounting information.

IT hardware/software: Includes, but is not limited to computers, internet access, remote access connections, email servers, file storage, webmail, smart phones, telephones, website, mobile phones etc.

3 General Principles

3.1 The Parish Clerk and all members should remain vigilant about cybersecurity threats. Suspicious activity or emails should be reported to the Parish Clerk.

3.2 IT resources and assigned council 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.

3.3 All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

3.4 Users should never share passwords via email and should be cautious of odd or inconsistent language in communications.

3.5 All users must comply with the council's Data Protection Document and Record Retention Policies.

3.6 Council devices must have up-to-date antivirus software, which must not be disabled without authorisation from the Parish Clerk.

3.7 Unauthorised use, modification, interference with computer systems or data is a breach of this policy and may be an offence under the Computer Misuse Act 1990.

3.8 Only properly licensed software may be installed on council devices, with the Parish Clerk's approval.

4 Training and Guidance

4.1 The Parish Clerk will receive appropriate cybersecurity training required for the role.

4.2 Members will be provided with a basic overview of cybersecurity measures when they join and may receive further guidance if required.

5 IT Provision and Policy

5.1 IT hardware, software, data access and services provided remain the property of the Parish Council and shall be recorded on the asset register.

5.2 At the end of any period of holding office, employment with or work for the Council, all equipment must be returned to the Clerk or Chair in full working condition. If equipment has been lost or damaged, or not returned within 14 days of leaving office, a charge may be made for its replacement or repair.

5.3 Users must comply with all relevant policies, procedures and UK legislation with respect to the use of IT hardware.

5.4 All IT provision should:

- Demonstrate value for use of Council money;
- Provide value for Council or clerk use, whilst enabling efficient working and not contributing to secondary waste;
- Include consideration of cost vs time spent carrying out tasks which could be offset by the use of technology;
- Maintain privacy of councillors, Council employees, subcontractors and parishioners in accordance with GDPR and the council's Data Protection and Document and Record Retention Policy;
- Adhere to other Council policies as much as is possible

5.5 A review of the Council's IT requirement should be conducted at least every four years, when council elections take place and new councillors take office, or within three months of new members of staff starting with the Council.

5.6 Hardware provided should only be used for Council business and not personal use.

Parish Clerk:

- The Parish Clerk will be assigned a council email address for official correspondence and is responsible for safeguarding any council devices, data, or systems under their control.

Members:

- Members will be issued council email addresses that should be the only address used for all council-related communications.
- Emails relating to council business are considered council data and may be subject to disclosure under the Data Protection Act or Freedom of Information Act, even when sent from personal accounts.
- Incoming emails to member accounts are stored on the server as per the Data Protection and Document and Record Retention Policies.
- When using social media in a personal capacity, members must make it clear they are not representing the Parish Council.
- Members must follow the Council's Code of Conduct when using social media.
- When using personal hardware to access Council systems or data, members are responsible for ensuring the security of systems and data.

6 Data management and security:

6.1 All sensitive and confidential 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.

6.2 Email accounts provided by the 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.

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

7 Websites and Social Media

7.1 The Parish Clerk shall ensure that the council website is accurate, up-to-date, and secure.

7.2 Council social media accounts may be managed by the Parish Clerk and, where applicable a delegated Councillor.

7.3 Posts on council-operated social media must remain non-political, factual, and in the interests of the parish.

7.4 Creation of new websites or social media accounts for council use requires Parish Clerk or council approval.

8 Password Protection

8.1 All council systems must be secured with passwords. Two-factor authentication should be enabled where possible. Unattended devices must be locked or require password re- entry.

8.2 Passwords must:

- Be at least eight characters long
- Include uppercase and lowercase letters, a number, and a special character
- Generic/shared accounts should be avoided.
- Access credentials must not be shared between users.
- Unique passwords should be used across different systems and devices.
- Passwords should be changed periodically.

9 Portable Devices

9.1 All mobile devices (phones, tablets, laptops) used for council business must be protected using passcodes, passwords, or biometric locks.

9.2 Removable media (such as USB drives) must be encrypted or password protected when containing sensitive council data.

10 Incident Reporting

10.1 Any incidents that may compromise council data or systems must be reported to the Parish Clerk without delay. This includes:

- Lost or stolen devices
- Phishing attempts
- Shared or compromised passwords
- Suspected unauthorised access

11 Misuse of IT

11.1 Misuse of IT systems is prohibited and may result in disciplinary or legal action. Misuse includes but is not limited to:

- Accessing, creating or sending offensive or inappropriate content
- Sending defamatory or infringing material
- Distributing spam or malware
- Interfering with others' data or work
- Changing system settings without permission
- Using council devices for gaming during work-related activities
- Unauthorised access to or distribution of council systems, data or information is strictly prohibited.

12 Risk Management

12.1 As part of its risk management the Council maintains insurance on the equipment provided.

12.2 All equipment must be secured from theft or unauthorised use as far as is practical. When travelling with equipment, it should not be left in an unattended vehicle unless there is no other option, in which case it should be secured out of sight.

12.3 Any loss of, or damage to equipment should be reported as soon as possible to the Clerk and Chair and any criminal damage will be reported to the Police by the Clerk.

12.4 Any loss of personal data as the result of loss or theft of equipment shall be reported to the Clerk and Chair and Information Commissioner's Office (ICO).

12.5 An annual risk assessment should be undertaken regarding use and security of Council IT hardware, software and stored data.