

Information Technology (IT) Policy

Parish Clerk | Email: clerk@kepc.info

1. Purpose

This IT Policy sets out how Kidmore End Parish Council (“the Council”) uses, manages, and protects its information technology systems and website. The policy ensures that digital services are secure, reliable, compliant with legal requirements, and used appropriately to support Council operations and public communication.

2. Scope

2.1 This policy applies to:

- All Parish Councillors
 - Council employees and contractors
 - Volunteers or third parties with access to Council IT systems
 - All devices used for Council business (Council-owned or personal)
 - The Parish Council website and associated digital services
-

3. Acceptable Use of IT Systems

3.1 Council IT systems must be used:

- For official Council business only
- In a lawful, ethical, and responsible manner
- In compliance with all relevant legislation and Council policies

3.2 Users must not:

- Access, store, or distribute inappropriate or unlawful content
- Use Council systems for personal financial gain or political activity
- Introduce malware or attempt to bypass security controls

3.3 Limited personal use may be permitted where it does not interfere with Council duties or system performance.

4. Website Management

4.1 The Parish Council website must:

- Provide accurate, up-to-date, and accessible information to the public
- Comply with UK accessibility regulations (WCAG 2.1 AA standard or latest applicable guidance)
- Be regularly reviewed and updated by authorised personnel

4.2 Content responsibilities:

- The Clerk (or designated officer) is responsible for overall website content
- Councillors may submit content, but publication must be approved
- All information must be factual, non-defamatory, and compliant with data protection laws

5. Data Protection and Privacy

The Council is committed to protecting personal data in accordance with applicable UK data protection legislation.

5.1 Key principles:

- Personal data must be processed lawfully, fairly, and transparently
- Data must only be collected for specified purposes
- Only necessary data should be retained
- Data must be kept accurate and secure

5.2 Users must:

- Not share personal data without proper authority
- Use secure methods when sending sensitive information
- Report any suspected data breach immediately to the Clerk

6. Information Security

6.1 To protect Council systems and data:

- Strong passwords must be used and not shared
- Devices must be locked when unattended
- Software must be kept up to date
- Antivirus and security measures must be maintained

6.2 Access to systems should be:

- Role-based (only what is necessary for duties)
- Removed promptly when no longer required

7. Email and Communication

7.1 Council email accounts must be used for official correspondence.

Users must:

- Maintain professionalism in all communications
- Be cautious of phishing emails and suspicious links
- Avoid sending confidential information unless secure methods are used

7.2 Emails may be subject to Freedom of Information (FOI) requests and must be retained appropriately.

8. Social Media and Online Presence

8.1 Where the Council uses social media:

- Accounts must be managed by authorised individuals only
 - Content must reflect the Council's official position
 - Personal opinions must not be presented as Council views
-

9. Backup and Continuity

- Website and critical data must be backed up regularly
 - Backups should be stored securely and tested periodically
 - The Council should have a basic disaster recovery plan to restore services in case of failure
-

10. Use of Personal Devices (BYOD)

10.1 If personal devices are used for Council business:

- They must meet minimum security standards
 - Council data must be kept separate where possible
 - Loss or theft must be reported immediately
-

11. Incident Reporting

11.1 All IT-related incidents must be reported promptly, including:

- Data breaches
- Lost or stolen devices

- Suspicious system activity

11.2 The Clerk will assess and take appropriate action.

12. Compliance and Monitoring

- The Council reserves the right to monitor IT usage where necessary
 - Breaches of this policy may result in disciplinary action
 - Serious breaches may be reported to relevant authorities
-

13. Review and Maintenance

13.1 This policy will be:

- Reviewed annually or when significant changes occur
 - Updated to reflect legal, technological, or operational changes
-