# IT Policy
# Aiskew and Leeming Bar Parish Council

Signed……

Adopted Date 15/10/2025

Review Date 15/10/2027

**1. Purpose**

This IT Policy outlines the standards for the use, management, and security of Information Technology (IT) systems and data at Aiskew and Leeming Bar Parish Council. It aims to:

1. Ensure effective and secure use of IT systems.
2. Protect council data and infrastructure.
3. Comply with UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.
4. Promote responsible use of digital communication and information.

**2. Scope**

This policy applies to all councillors, employees, contractors, and volunteers who use or access the council's IT systems, data, or digital communication tools.

**3. IT Equipment and Services**

1. The Parish Council may provide councillors and staff with devices (e.g. laptops, tablets) where necessary.
2. All devices must be password protected, regularly updated, and used primarily for council business.
3. Personally owned devices used for council work must comply with the same security measures.

**4. Email and Communication**

1. Official council business must be conducted through designated council email addresses.
2. Personal email accounts must not be used for council work.
3. All communication should be professional, respectful, and in line with the council's Code of Conduct.
4. Sensitive information must be encrypted or securely transmitted.

**5. Data Protection and Privacy**

1. The Council is committed to full compliance with the UK GDPR.
2. Personal data must be stored securely, only accessible to authorised individuals.
3. Data must not be shared without appropriate consent or legal basis.
4. Any data breaches must be reported immediately to the Clerk and may be subject to ICO notification.

**6. Website and Social Media**

1. The Council's website is managed by the Clerk or designated webmaster and must comply with accessibility standards (WCAG 2.1 AA).
2. Social media accounts representing the Council must be used responsibly to share factual and helpful information.
3. Personal opinions must not be expressed on official council platforms.

**7. Software and Updates**

1. Only licensed and approved software may be installed on council devices.
2. All systems should be kept up to date with the latest security patches and updates.
3. Antivirus software must be active and regularly updated.

**8. Backups and Recovery**

1. Council data (including meeting minutes, financial records, and correspondence) must be backed up regularly.
2. Backup copies should be stored securely and separately from primary systems.
3. The Clerk is responsible for ensuring that a disaster recovery plan is in place.

**9. Remote and Home Working**

1. Staff and councillors working from home must ensure a secure working environment.
2. Devices must not be left unattended or accessible by unauthorised individuals.
3. Confidential documents should not be printed or disposed of in unsecured home settings.

**10. Misuse and Disciplinary Action**

1. Misuse of IT systems includes unauthorised access, inappropriate communication, or intentional breach of security.
2. Any misuse may result in disciplinary action, referral to external authorities, or both.

**11. Roles and Responsibilities**

1. The Clerk is the designated Data Protection Officer (DPO) and IT coordinator.
2. All users are responsible for adhering to this policy and reporting any concerns or breaches.

**12. Review and Amendments**

This policy will be reviewed annually or when significant changes in technology or legislation occur.