



Aldeby Parish Council IT Policy

1. Introduction

Aldeby parish council recognises the importance of effective and secure information technology (IT) and email usage 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.

2. Scope

This policy applies to all individuals who use Aldeby parish council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Aldeby parish council IT resources and 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. 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 Aldeby parish council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

5. Data management and security

All sensitive and confidential Aldeby 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. Backups are undertaken monthly, using children, parent, grandparent backups. External drive is stored off site, at the Clerks house.

6. Network and internet usage

The Clerk working for Aldeby parish council uses a secure internet at home.

7. Email communication

Currently there are no gov.uk secure email addresses. This will be looked at and a service will be provided to resolve this.

8. Password and account security

Aldeby 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. The Proper Officer's password will be stored in a sealed envelope signed over the seal and given to the Chair for safe keeping.

9. Mobile devices and remote Work

No mobile devices are provided by Aldeby parish council. However, the Clerk has a 'work' mobile phone which is secured with passcodes and biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

10. Email monitoring

Aldeby parish council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and UK GDPR. Please refer to the Aldeby Data Protection policy. At no point should personal emails be used for parish council business.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox. Please refer to the Aldeby Retention of Documents Policy.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Proper Officer for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately and notify James Shore for email concerns.

13 Training and awareness

Aldeby parish council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

14. Website Compliance

[Aldeby parish council](#) website needs to be a gov.uk domain. Although this needs to be done, the Clerk checks Aldeby parish council files uploaded to this website is accessibility compliant and that the website itself is WCAG2.2AA compliant and will be reviewed regularly.

15. Compliance and consequences

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

16. 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.

17. Contacts

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

All staff and councillors are responsible for the safety and security of Aldeby parish council's IT and email systems. By adhering to this IT Policy, Aldeby parish council aims to create a secure and efficient IT environment that supports its mission and goals.

Date: _____

Signature: _____

Role: _____

Reviewed and adopted: 5th November 2025
Review September 2026