# Aust Parish Council

# IT and Email Policy

| Version | Date adopted | Minute ref: | Details / Key Changes | Review due |
|---|---|---|---|---|
| 1.0 | 10/06/2025 | 2025-06-8.2 | First adoption. Based on template policy provided by the Smaller Authorities Proper Practices Panel | June 2027 |

## 1. Introduction

Aust 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 and employees.

## 2. Scope

This policy applies to all individuals who use Aust Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts. It also applies to councillors when using private email accounts in their capacity as councillors.

## 3. Acceptable use of IT resources and email

Aust 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.

Users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content. This also applies to the use of private email accounts for council business.

## 4. Device and software usage

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

## 5. Data management and security

All sensitive and confidential data should be stored and transmitted securely using approved methods. Files on the main council laptop should be backed up via cloud storage, currently OneDrive.

Staff and councillors should ensure that any personal devices used to access council records (including emails) have appropriate security features enabled, including a password, PIN or biometric lock.

Usage of virus-tracking and firewall software is compulsory on council-owned devices, and strongly recommended for other devices used for council business.

**6. Internet usage**

Internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

**7. Email communication**

Email accounts provided by Aust Parish 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.

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

**8. Password and account security**

Aust Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. The passwords and account details for council accounts are stored in the LastPass secure password management system, to which the Clerk and Chair hold the master password.

**9. Mobile devices and remote work**

Mobile devices used for council business should be secured with passcodes and/or biometric authentication. Users should ensure that the devices are kept in a secure location whenever possible and that they are closely monitored when being used outside the normal place of work.

**10. Email monitoring**

Because councillors use privately owned email accounts, Aust Parish Council has no ability to monitor traffic through those accounts in relation to GDPR compliance, Freedom of Information requests or general council business. Councillors are required to co-operate with any such investigations and to provide copies of all relevant emails from their private accounts.

**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.

**12. Reporting security incidents**

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact (the Clerk) for investigation and resolution.

**13 Training and awareness**

All employees and councillors will receive an annual briefing on email security and best practices.

**14. Compliance and consequences**

Breach of this IT Policy may result in consequences as deemed appropriate.

## 15. Policy review

This policy will be reviewed every two years to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

## 16. Contacts

For IT-related enquiries or assistance, users can contact the Clerk

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