ALVANLEY PARISH COUNCIL INFORMATION TECHNOLOGY (IT) AND EMAIL USE POLICY

1. Introduction

Alvanley Parish Council ("the Council") relies on secure and effective information technology to support its operations, decision-making, and communication.
This policy sets out the standards, responsibilities, and procedures for the appropriate use of IT systems, devices, data, and email by councillors, employees, volunteers, and contractors ("users").

The aims of this policy are to:

- protect the Council's information and systems
- ensure compliance with legal and regulatory obligations
- promote safe, responsible, and professional use of technology

2. Scope

This policy applies to all individuals who access or use:

- Council-owned computers, phones, tablets, and other devices
- personal devices used for Council business (BYOD)
- Council email accounts
- Council data, documents, and digital records
- Council-funded software, cloud services, and online platforms

All users must comply with this policy to maintain digital security and protect personal data.

3. Roles and Responsibilities

The Council

- Provides approved devices, software, and secure storage solutions where possible
- Ensures policies and procedures are in place
- Reviews this policy annually

The Clerk

- Acts as the primary IT contact
- Maintains Council accounts, email systems, and access permissions
- Ensures backups and data retention processes are followed
- Coordinates responses to Freedom of Information (FOI) and Subject Access Requests (SARs)

Data Protection Officer (DPO The Council)

- Provides guidance on GDPR compliance
- Advises on data breaches and reporting obligations

All Users

- Follow this policy and all related procedures
- Protect Council data and devices
- Report incidents promptly
- Use Council systems professionally and responsibly

4. Training and Awareness

The Council will provide or signpost regular training, including:

- National Cyber Security Centre (NCSC) Cyber Security Training for Small Organisations
- NCSC Cyber Action Toolkit
- Email security and phishing awareness

Users are expected to engage with training and keep their knowledge up to date.

5. Acceptable Use of Council IT Resources

When using Council-owned devices or systems, users must:

- use them only for legitimate Council business
- comply with copyright and intellectual property law
- use only authorised software and applications
- keep devices secure and report faults promptly
- avoid accessing, storing, or forwarding inappropriate or offensive content

Users must not install software or apps without approval from the Clerk.

6. Use of Personal Devices (BYOD)

Where personal devices are used for Council business, users must:

- use strong, unique passwords (preferably via a password manager)
- keep operating systems and apps updated
- use reputable anti-virus software

- ensure devices are protected by a screen lock
- avoid shared family devices for Council work
- store Council data only in approved locations (e.g., Council-managed cloud storage)

If a user leaves the Council, all Council data must be deleted from personal devices.

7. Network and Internet Usage

Users must:
- avoid public or unsecured Wi-Fi for Council business
- use trusted, password-protected networks
- use a VPN if accessing sensitive information remotely (where provided)

8. Password and Account Security

Users must:
- follow NCSC guidance for creating strong passwords
- never share passwords with others
- store emergency access details securely for business continuity
- use multi-factor authentication (MFA) where available

The Clerk may hold sealed access credentials for emergency use only.

9. Email Communication

The Council will provide official email accounts for all councillors and staff.
Users must:
- use Council email accounts for all Council business
- maintain a professional and respectful tone
- check recipients carefully before sending sensitive information
- be cautious with attachments and links
- verify suspicious emails before opening them

Personal email accounts used for Council business remain subject to FOI (Freedom of Information) , SAR (Subject Access Request) and GDPR obligations.

10. Email and Account Access

The Council reserves the right to access Council email accounts:
- to ensure compliance with this policy
- to respond to FOI or SAR requests
- for business continuity

Any monitoring will comply with the Data Protection Act and GDPR.

11. Data Storage, Retention, and Security

Users must:

- store Council data only in approved locations (e.g., OneDrive, SharePoint)
- avoid storing Council data on personal hard drives or USB sticks unless encrypted
- follow the Council's Data Retention Schedule
- archive or delete emails in line with retention requirements
- ensure regular backups are completed (managed by the Clerk)

Sensitive or confidential data must be encrypted when stored or transmitted.

12. Use of Messaging Apps and Social Media

Council business must not be conducted via:

- Facebook Messenger
- SMS
- Personal social media accounts

These platforms are not compliant with GDPR for official communications.

13. Starters, Leavers, and Change of Role

When a user joins the Council

- accounts and access permissions will be created
- training will be provided

When a user leaves the Council

- Council devices must be returned
- Council email accounts will be closed
- all Council data must be removed from personal devices
- access permissions will be revoked

14. Reporting Security Incidents

Users must immediately report:

- suspected data breaches
- lost or stolen devices
- suspicious emails or malware
- unauthorised access to accounts or systems

Reports should be made to: The Clerk of the Parish Council

The Clerk and DPO will assess whether the ICO must be notified.

15. Compliance and Consequences

Failure to comply with this policy may result in:

- suspension of IT access
- referral to the Monitoring Officer
- disciplinary action (for employees)

Serious breaches may result in legal consequences under GDPR or other legislation.

16. Policy Review

This policy will be reviewed annually or sooner if:

- legislation changes
- new risks emerge
- new systems or technologies are introduced

17. Contacts

For IT support or queries: The Clerk of the Parish Council
For data protection matters: The Clerk of the Parish Council

Adopted: 15th April 2026

Next Review Date: April 2027