

ASTLEY PARISH COUNCIL

IT, Email and Mobile Device Policy

1. Introduction

This policy sets out the arrangements for the safe and appropriate use of the Council's information technology equipment.

The Council recognises its obligations under the Data Protection Act 2018 and the UK General Data Protection Regulation and will take proportionate steps to protect information held electronically.

This policy applies to:

- One Council-owned laptop computer
 - One Council-owned basic mobile telephone (incoming calls and SMS only)
 - The Council's official email account(s)
-

2. Council-Owned Laptop

2.1 Purpose

The laptop is provided for the administration of Council business, including:

- Preparation of agendas and minutes
- Financial administration
- Email correspondence
- Storage of Council documents

It shall not be used for personal purposes.

2.2 Ownership and Responsibility

- The laptop remains the property of the Council.
 - It is issued to the Clerk (or named officer role).
 - The Clerk is responsible for its safe custody and appropriate use.
-

2.3 Security Measures

The following minimum safeguards shall be in place:

- Password-protected login
- Up-to-date antivirus software
- Operating system updates enabled
- Firewall enabled
- Automatic screen lock after a short period of inactivity

The device shall not be shared with family members or third parties.

2.4 Storage and Handling

- The laptop shall be stored securely when not in use.
 - It must not be left unattended in public places.
 - When transporting the device, reasonable care must be taken to prevent theft or damage.
-

2.5 Backups

Council documents shall be backed up regularly using:

- Secure cloud storage, or
- Encrypted external storage device

Backups shall be retained securely and separately from the laptop where possible.

3. Council Email

3.1 Official Use

Council business must be conducted through the Council's official email account, not personal email accounts wherever possible.

3.2 Email Security

- Strong passwords shall be used.
- Passwords shall not be shared.
- Suspicious emails or attachments must not be opened.
- Personal data shall only be shared where necessary and lawful.

3.3 Record Keeping

Emails forming part of Council decisions or administration shall be retained in accordance with the Council's document retention practices.

4. Basic Mobile Telephone (Incoming Calls and SMS Only)

4.1 Purpose

The Council maintains one basic mobile telephone to receive incoming calls and text messages relating to Council business.

The device:

- Cannot access the internet
 - Cannot access Council systems
 - Is not used for outgoing calls
-

4.2 Acceptable Use

- The phone is for Council business only.
 - Sensitive or confidential information should not be requested or stored via SMS.
 - Relevant communications shall be recorded appropriately in Council records.
-

4.3 Data Protection

- Personal data received by text shall only be retained where necessary.
 - Messages containing personal information shall be deleted once recorded appropriately.
 - Voicemail messages containing personal data shall not be retained longer than necessary.
-

4.4 Security

- PIN protection shall be enabled (where supported).
- The phone shall be kept securely by the Clerk (or designated officer).

- Loss or theft must be reported immediately to the mobile provider for SIM cancellation.
 - The Chair shall be informed.
-

5. Loss, Theft or Data Breach

If Council equipment is lost, stolen, or believed to be compromised:

- The incident shall be reported immediately to the Chair.
 - Appropriate steps shall be taken to secure accounts and cancel SIM services.
 - Consideration shall be given as to whether a personal data breach has occurred and whether reporting is required.
-

6. Review

This policy shall be reviewed periodically and updated as necessary.

Adoption

Resolved:

That this IT, Email and Mobile Device Policy was approved by Parish Council at a meeting held on:

Date: _____

Minute Reference: _____

Signed: _____

Chair of the Council

Signed: _____

Clerk / Responsible Financial Officer

Review Date: _____