Alstonefield Parish Council IT, GDPR & BYOD Policy (2026)

1. Policy Statement

Alstonefield Parish Council ("the Council") is committed to protecting personal data and ensuring compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Data (Use and Access) Act 2025 (and 2026 guidance updates)
- WCAG 2.2 AA standards as required by the 2018 Accessibility Regulations

The Council recognises it acts as a Data Controller in most cases.

Personal data shall be processed in accordance with the core principles of UK GDPR: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and security.

2. Scope

This policy applies to:

- All parish councillors
- The Clerk
- Any contractors or volunteers
- All personal data in electronic or paper form

3. Proportionate Approach (Small Council Context)

Given the Council:

- Owns no buildings
- Uses one council-owned laptop with cloud-based data backup
- Has limited processing activities

The Council adopts a risk-based, proportionate compliance model, ensuring safeguards are appropriate to the scale of processing.

4. IT & Information Security Policy

4.1 Council Equipment

- The Council maintains one official laptop, which:
    - Must be password protected
    - Must use full disk encryption (e.g. BitLocker/FileVault)
    - Must have automatic updates enabled
    - Must run antivirus software
- The laptop must not be shared with non-council users.

4.2 Storage of Data

- Council data must be stored:
    - On the council laptop or
    - In an approved secure cloud service
- Council data must not be stored permanently on USB sticks or personal devices.

4.3 Email Use

Currently only the clerk has a council owned email account/address. We are working towards compliance with the following paragraph and should be compliant by July 2026.

All council business must be conducted via official council email accounts. Use of personal email for council business is prohibited to ensure compliance with FOI and GDPR data-retrieval requirements.

4.4 Backups

- Data must be backed up regularly (e.g. cloud sync or encrypted backup)
- Backup access must be restricted

4.5 Incident Reporting

All data breaches must be reported immediately to the Clerk (or Chair if no Clerk).

The Council will assess whether the breach must be reported to the ICO within 72 hours.

4.6 Website

The Clerk will ensure the Council website remains compliant with current accessibility regulations and that an Accessibility Statement is reviewed annually.

5. GDPR Compliance Policy

5.1 Lawful Basis for Processing

The Council will process personal data under lawful bases such as:

- Public task (most council functions)
- Legal obligation (e.g. elections, finance)
- Consent (where required)

The Council will not rely on legitimate interests where acting as a public authority.

5.2 Data Minimisation

The Council will only collect data that is:

- Necessary
- Relevant
- Proportionate

5.3 Transparency

The Council will maintain a Privacy Notice explaining:

- What data is collected
- Why it is collected
- How long it is kept

- Who it is shared with

5.4 Data Subject Rights

Individuals have the right to:

- Access their data
- Rectify inaccuracies
- Request erasure (where applicable)
- Restrict processing
- Object to processing

The Council will respond to requests within one month.

5.5 Data Retention

The Council will:

- Maintain a simple retention schedule
- Delete data when no longer required
- Securely destroy paper and electronic records

5.6 Data Sharing

Data will only be shared:

- Where legally required
- With appropriate safeguards
- With formal agreements where necessary

5.7 Accountability

The Council will:

- Keep basic records of processing activities
- Review policies annually
- Ensure councillors understand responsibilities

6. Bring Your Own Device (BYOD) Policy

Because councillors may use personal devices, the following rules apply:

6.1 Permitted Use

Councillors may use personal:

- Phones
- Tablets
- Laptops

to access council email or documents.

6.2 Minimum Security Requirements

All personal devices used for council business must:

- Be password or biometric protected
- Automatically lock after inactivity
- Have up-to-date software
- When using personal devices in public places, Councillors are encouraged to be mindful of their surroundings and to use secure, password-protected Wi-Fi connections where available. The use of mobile data (4G/5G) is recommended as a more secure alternative to open, unencrypted public Wi-Fi.Use Multi-Factor Authentication (MFA) where the service provider supports it (e.g., for accessing council email/cloud storage)
- All personal mobile devices used to access council email must have a secure screen lock (PIN, password, or biometrics) enabled. Councillors must ensure that 'Device Encryption' is active (this is standard on most modern smartphones once a screen lock is set).

6.3 Data Handling

- Personal data must not be permanently stored on BYOD devices
- Access should be via secure cloud/email systems where possible

- Downloads should be deleted when no longer required

6.4 Loss or Theft

If a device is lost or stolen:

- The councillor must report it immediately
- The Council will assess risk and take action

6.5 Email & Messaging

- Avoid using WhatsApp/SMS for personal data unless necessary
- Do not share sensitive data via informal channels

6.6 Leaving Office

When a councillor or clerk leaves:

- All council data must be deleted from personal devices
- Upon resignation, all council-held digital credentials (passwords, admin rights) must be transferred to the Chair/Successor within 7 days, and council data must be wiped from personal devices
- Access to council systems must be removed

7. Records & Documentation

The Council will maintain:

- Privacy Notice
- Retention Schedule
- Basic Data Audit (simple spreadsheet is sufficient)
- Breach Log (if applicable)

8. Data Protection Officer (DPO)

The Council is not required to appoint a DPO but will:

- Assign responsibility to the Clerk or Chair

- Ensure compliance oversight

9. Review

This policy will be:

- Reviewed annually
- Updated following legal or operational changes

10. Adoption

Adopted by: Alstonefield Parish Council

Date: 08/04/2026

Review Date: 01/05/2027