ALMONDSBURY
PARISH COUNCIL

I.T. AND DATA MANAGEMENT POLICY

1. Purpose

This policy sets out how Almondsbury Parish Council manages and safeguards its information technology (I.T.) systems, data, and digital communications to ensure the integrity, security, and lawful use of council information and finances, in line with **b** of the Annual Governance and Accountability Return (AGAR).

It supports effective governance, financial management, and compliance with data protection and transparency requirements.

2. Scope

This policy applies to:

- All councillors, employees, and contractors who have access to the Council's I.T. systems, emails, or data.
- All digital devices, systems, and online platforms used by the Council.
- All data processed, stored, or transmitted in connection with Council business, including financial, administrative, and personal information.

3. Objectives

The Council aims to:

- Ensure that its I.T. systems are reliable, secure, and fit for purpose.
- Protect data from loss, damage, misuse, or unauthorised access.
- Maintain accurate and accessible electronic financial records.
- Comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Local Government Transparency Code.
- Support business continuity and effective decision-making.

4. I.T. Systems and Access Control

- All computers, laptops, and other devices used for Council business must be password-protected.
- Access to Council systems is restricted to authorised users only.
- Usernames and passwords must not be shared, except for the Chair having a sealed envelope containing all passwords.
- Systems containing financial or personal data must use strong passwords and, where possible, two-factor authentication.

- Access rights will be reviewed annually and revoked when no longer required.

5. Data Storage and Backup

- All official Council documents and data must be stored in secure locations — either on Council-managed devices or approved cloud storage systems (e.g. OneDrive, SharePoint, or equivalent).
- Data backups will be taken regularly and stored securely to allow recovery in case of system failure or data loss.
- Paper and digital records must be retained or disposed of in accordance with the Council's Document Retention Policy.

6. Email, Internet and Software Use

- The Council's official email address (e.g. clerk@almondsburyparishcouncil.gov.uk) must be used for all official correspondence.
- Personal email accounts must not be used for Council business.
- Only authorised software shall be installed on Council devices.
- Councillors and staff must take care to avoid phishing or fraudulent emails and report any suspected cyber incidents immediately to the Clerk and Chair.

7. Financial Systems and Controls

- Financial records are maintained on approved accounting software or spreadsheets under the control of the Responsible Financial Officer (RFO).
- Regular backups and reconciliations are undertaken in accordance with Financial Regulations.
- Electronic banking is restricted to authorised signatories, and dual authorisation must be used.
- Audit trails are maintained for all electronic financial transactions.

8. Data Protection and Privacy

- The Council is registered with the Information Commissioner's Office (ICO).
- Personal data will be collected, processed, and stored in accordance with the Council's Privacy Notice and GDPR Policy.
- Councillors and staff will receive basic data protection awareness training.

9. Incident Reporting and Business Continuity

- Any I.T. failure, data breach, or suspected cyberattack must be reported immediately to the Clerk and Chair.
- The Clerk will ensure appropriate remedial and reporting actions are taken, including notification to the ICO where required.
- The Councils Business Continuity Plan will ensure that essential services and financial operations can continue in the event of an I.T. disruption.

10. Review and Monitoring

- This policy will be reviewed annually alongside the Council's Financial Regulations and risk assessments.
- The Internal Auditor will verify that the Council has effective I.T. and data management arrangements in place in line with Assertion 10.

Adopted at the Full Council Meeting 05.03.26
Review date: May 2027