**Allostock Parish Council**

**Information Technology (IT) Policy**

1.Introduction

This Information Technology Policy establishes the standards, responsibilities and procedures for the secure and effective use of digital systems within the Parish Council. It ensures compliance with statutory requirements, including the Annual Governance and Accountability Return (AGAR) Assertion 10, the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2.Purpose

The purpose of this policy is to

- Protect council data and digital assets
- Ensure responsible and lawful use of IT systems
- Provide clear guidance to 10, the and volunteers.
- Maintain transparency, accessibility, and cybersecurity standards.

3.Scope

This policy applies to all individuals who access or process council information using:

- Council owned devices
- Personal devices used for council business (BYOD)
- Council email accounts
- Cloud storage and software services
- The council website and social media accounts
- Any digital communication platform used for council business

4. Roles and responsibilities

4.1 Councillors and staff

- Use IT systems responsibly and only for legitimate council business
- Protect council data and report incidents immediately
- Follow guidance data protection and cybersecurity guidance

4.2 Clerk (System administrator)

- Manage user accounts
- Maintain council website and ensure accessibility compliance
- Oversee GDPR compliance and data protection procedures

4.3 IT Support

- Maintain devices and software
- Ensure security patches and anti/virus protection are up to date.
- Assist with incident response and system troubleshooting.

5.Acceptable use

- Council IT resources must be used solely for council related activities

- Personal use of council owned devices must be minimal
- Users must not install unauthorized software or access inappropriate content
- All official communication must use council approved email accounts

6. Device Security

6.1 Council owned devices

- Must be password protected and regularly updated
- Must have anti-virus and security patches enabled
- Must be returned to the clerk at the end of office or employment

6.2 Personal Devices (BYOD)

- Allowed only with clerk approval
- Must use secure passwords and updated software
- Must not permanently store council data

7.Data Protection

- All personal data must be processed in accordance with UK GDPR AND THE Data Protection act 2018
- Data must be stored only in approved locations
- Confidential information must not be share via unsecured channels
- Regular back ups must be performed and monitored

8 Email and Communication

- All council business must use council approved email accounts
- Messaging apps may be used only for operational coordination not decision making
- Important messaged must be forwarded to the clerk's email for record keeping

9 Password and Authentication

- Password must be strong (minimum 12 characters, mixed types)
- Passwords must not be shared
- Multi factor authentication must be used where available

10 Cybersecurity

- Users must be trained to recognize strong (and suspicious activity)
- Software updates must be installed promptly
- Antivirus software must be active on all devices
- Any suspected breach must be reported immediately to the clerk

11. Website and Accessibility

- The clerk or appointed webmaster is responsible for maintain the Council website
- The website must meet accessibility standards
- Content must be accurate, up to date and compliant with transparency regulations

12 Data Handover and Exit procedures

When a councillor or staff member leaves:

- All council data must be returned or transferred.
- Access to accounts must be revoked immediately
- Personal devices must have council data removed

13 Policy Review

This policy must be reviewed annually and re-adopted by the council to remain compliant with AGAR Assertion 10.

14.Adoption

This information technology report was reviewed and adopted by the Parish Council at its meeting held on 24/09/26 and will be reviewed annually to ensure compliance with relevant legislation.