Plaistow and Ifold Parish Council IT Policy

1. Purpose

This policy outlines the acceptable use, management, and security of IT resources provided by Plaistow and Ifold Parish Council. Its aim is to ensure that technology is used responsibly and in alignment with legal, ethical, and operational standards.

2. Scope

This policy applies to all councillors, employees, contractors, and volunteers who use Council IT resources, including hardware, software, networks, and data systems.

3. Data Security and Confidentiality

- All personal and sensitive data is considered confidential and must be handled with appropriate care in accordance with GDPR and *SAPP Assertion 10 Digital and Data Compliance for Councils. The Clerk and Council recognise their role as both data controllers and data processors.
- Users must not disclose personal or sensitive information without proper authorisation.
- Devices must be password-protected, and access credentials must not be shared. Multi Factor Login for Clerk and Councillor Emails is recommended.

4. Acceptable Use

- IT resources are to be used for Council business only.
- Personal use is permitted where reasonable and does not interfere with operations.
- Users must not install unauthorized software or connect unauthorized devices.

5. Internet and Email

- Email communication must be professional and relevant to Council matters.
- Users must not access, transmit, or store material that is offensive, illegal, or inappropriate.
- Social Media communication must be professional and relevant to Council matters.

6. Software Management

- All software used must be legally licensed and approved by the Council.
- Updates and security patches must be installed promptly.
- Users are prohibited from copying or distributing software without permission.
- The Plaistow and Ifold Website must adhere to the Accessibility requirements for Parish Councils in accordance with *SAPP Assertion 10: Digital & Data Compliance for Councils. (See Accessibility Statement WCAG 2.2 AA is a requirement)

7. Equipment and Asset Care

- Devices and equipment must be handled responsibly and securely.

- Loss or damage of equipment must be reported immediately to the Council Clerk or Full Council.
- Council-owned devices remain property of the Council and must be returned promptly if an individual leaves their role.

8. Cybersecurity

- Antivirus and security systems must be active on all Council devices.
- Users must report any suspected security breach or phishing attempt to Full Council or the Clerk.
- Passwords must be changed regularly and follow complexity requirements.

9. Backup and Data Retention

- Important Council data must be backed up daily.
- Data retention will follow current legal standards including GDPR and in accordance with *SAPP Assertion 10 Digital and Data Compliance for Councils (see Retention of documents Policy)
- Obsolete data must be securely deleted or securely archived (if there is no requirement to destroy).

10. Policy Enforcement

- Failure to comply may result in disciplinary action, including revocation of access.
- This policy will be reviewed annually to ensure ongoing relevance and effectiveness.

Adopted by Plaistow and Ifold Parish Council xxxxxxxxxxxxx

*Smaller Authorities' Proper Practices Panel SAPP Assertion 10:

The key requirements are:

1. Council-owned domain names for websites and email
2. Website accessibility compliance with WCAG 2.2 AA
3. IT policies for all smaller authorities
4. Proper data protection practices:
   In particular

— Comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
— Process personal data lawfully, fairly, and in line with UK GDPR principles
— Recognise their roles as both a Data Controller and a Data Processor. A data controller determines the purposes and means of the processing of personal data. A processor engages in personal data processing on behalf of the controller.