INFORMATION TECHNOLOGY POLICY – approved 18 MAR 2024

(to be reviewed/updated by 1 March 2025)

1. Purpose:
This IT Policy is established to ensure the proper and secure use of information technology resources within the Parish Council. It outlines the guidelines, procedures, and responsibilities to safeguard information, promote efficient technology use, and maintain a secure computing environment.

2. Governance & Scope:
This policy applies to all Councillors, employees, contractors, volunteers, and any other individuals granted access to Parish Council information technology resources.

Roles and responsibilities for IT management and support and to oversee the implementation of new services must be established. Those who hold these roles and responsibilities must demonstrate competence in these matters. Proper management and control of systems and best use of equipment and services will form part of the council's annual risk assessment and review.

It will be the responsibility of staff and councillors who manage the council's IT systems to identify and implement suitable training measures to be fully equipped to discharge their responsibilities.
All such training will be at the Council's expense.

Use of a third party to manage and maintain the council's IT environment is acceptable provided that credentials have been established and a formal contract setting out terms of reference is held. This should include a declaration of confidentiality.

Plans must be established and kept under review setting out the council's IT goals.
Given the fast changing nature of the IT sector the council will welcome new innovations as and when they suit its requirements. Notwithstanding which, the policy must be reviewed at least annually.

3. Acceptable Use:
3.1. Parish Council IT resources are to be used for official purposes only. Personal use is not permitted.
3.2. Users must comply with all applicable laws and regulations while using IT resources, and specific attention is drawn to the Council's own GDPR policy.
3.3. Unauthorised access, use, or distribution of Parish Council data is strictly prohibited.

4. Information Security:
4.1. Users must protect their login credentials and not share them with others.
4.2. All computing devices used to access the council by web or email must have up-to-date antivirus software and security patches. This also applies to councillor's personal devices used to access Council data.
4.3. Encryption should be used for sensitive data, especially when transmitted over the internet.
4.4. Lost or stolen devices containing Parish Council data must be reported immediately to the clerk.
4.5. Parish Council information/data must not be stored on devices not owned by the council. The council will provide space for individual councillors and staff on its servers for this purpose*. (NB March 2024 until such space is made available extreme care must be exercised to ensure that council information does not fall into the wrong hands*)
4.6. Councillors who use a shared device to access Parish Council resources must log out after use. "Remember me" usernames and passwords to enter council sites must be disabled. They should always be aware of their immediate environment taking care to ensure that information displayed on screens is not disclosed inadvertently.

5. Data Management:
5.1. Parish Council data should be classified based on sensitivity (see also section 10), and access should be granted on a need-to-know basis.

5.2. Apart from the clerk and staff requiring access in the normal course of work, it is recognised that councillors have a right to access any information held by the council when it is relevant to the work assigned to them. An exception to this will be employee information which is restricted to members of the Employment committee.
5.3. Councillors obtaining access (on the basis of 5.1. and 5.2.) will do so on a "read only" basis and must be used strictly in connection with Council business. Any such access is to be reported to the clerk within 24 hours detailing what information was sought, the reason why. The clerk will maintain this information as part of the normal retention of records protocol.
5.4. Data backups must be performed daily to prevent data loss and restoration tested weekly.
5.5. Data retention and disposal policies should be followed to comply with relevant regulations.
5.6. It will be the responsibility of the clerk to ensure that safety and security of council data is maintained at all times.

6. Internet, Email Usage:
6.1. Internet use is for work-related activities. Inappropriate or excessive use is prohibited.
6.2. Email communication should adhere to professional standards. Users must be cautious of phishing attempts and report any suspicious emails.
6.3. Parish Council email accounts are for official business, and not for personal use.
6.4. Private email accounts must not be used for Parish Council business (see also 7 below).

7. Non Corporate Channels
Includes – private email accounts, private messaging (e.g. WhatsApp), direct messages (e.g. X, Facebook), private mobile devices (text and voice messages).
7.1. Use of these channels should be restricted comments of a general nature (see 7.2)
7.2. If any conversation drifts into official business, it must be transferred into the Parish Council's email system for retrieval later if required.
7.3. No Parish Council data may be transferred out using any of this type of media.
7.4. The Code of Conduct shall continue to apply throughout

8. Software and Hardware:
8.1. Only authorised software should be installed on Parish Council computers.
8.2. Employees should not attempt to repair or modify IT equipment without approval from the clerk
8.3. Personal devices connected to the Parish Council network must comply with security standards.
8.4. It will be the responsibility of the clerk to seek support and advice and to install suitable technical controls to protect the council from cyber security attacks, including firewalls, secure configuration, access control, malware protection and patch management.
8.5. The clerk must ensure that in the event of data or equipment loss/malfunction or staff incapacity the business as usual can prevail.

9. Social Media:
9.1. Councillors and Employees must use social media responsibly, avoiding disclosure of confidential information related to Parish Council matters.
9.2. Refer to the social media policy contained within the Community Engagement Policy for more detail.

10. Freedom of Information Act 2000, Section 46
10.1. The council will review policies and procedures at least annually to ensure compliance with the code.
10.2. Council systems will be made available to the Information Commissioner upon request for inspection and assessment as to whether good practice is followed.

11. Training and Awareness:
11.1. Employees and councillors will receive initial training on IT policies and security best practices, and it will be a requirement to keep their knowledge up to date through regular reading and viewing (RRV) which will be provided by the clerk.

11.2. The clerk will conduct awareness campaigns to keep users informed about emerging threats.

12. Enforcement:
12.1. Violations of this policy may result in disciplinary action, including but not limited to verbal or written warnings, suspension of IT privileges, or suspension/termination of employment.
Similar sanctions may apply to councillors if a complaint has been raised by way of a violation of the Code of Conduct

13. Review and Revision:
This policy will be reviewed at least annually and updated as necessary to ensure its effectiveness and relevance.

Approved by the Council [Date]