



INFORMATION TECHNOLOGY (IT) POLICY

1. Introduction

1.1 This Information Technology (IT) Policy sets out how the Parish Council uses and protects its IT systems and information.

1.2 The policy is proportionate to the size of the Council, which has one employee and one council-owned laptop. Councillors use their own personal devices to access council information and must full comply with data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1.3 This policy is informed by and aligned with good practice guidance issued by the National Association of Local Councils (NALC), the Society of Local Council Clerks (SLCC), and the National Cyber Security Centre (NCSC).

2. Purpose

2.1 The purpose of this policy is to:

- protect the Parish Council's information and digital assets;
- set clear expectations for acceptable IT use;
- reduce the risk of data loss or cyber security incidents; and
- support compliance with data protection legislation.

3. Scope

3.1 This policy applies to:

- the Parish Council's employee; and
- all councillors when accessing council information.

3.2 The policy applies regardless of location, including when working from home or remotely.

4. Council-Owned Equipment

4.1 The Council provides one laptop for official council business.

4.2 The employee must:

- use the laptop primarily for council business;

- take reasonable care to prevent loss, theft or damage;
- ensure the laptop is password protected;
- lock the device when not in use; and
- not install software or hardware without authorisation
- make regular back ups council documents on the external hard drive

4.3 Any faults, loss, or damage must be reported to the Chair as soon as possible.

5. Use of Personal Devices (Councillors)

5.1 Councillors may use their own personal devices (such as laptops, tablets or smartphones) to access council emails and documents.

5.2 When doing so, councillors must:

- use a secure password, PIN or biometric protection;
- keep device software up to date;
- ensure council information cannot be accessed by others; and
- use a dedicated council email account for council business; all official council business is conducted solely via the clerk and the official council email address.

5.3 Parish council information should not be stored unnecessarily on personal devices and should be deleted when no longer required.

6. Passwords and Security

6.1 Passwords must be strong and must not be shared.

6.2 The use of three random words is recommended, in line with NCSC guidance.

6.3 Multi-Factor Authentication (MFA) should be enabled where available.

6.4 Passwords must be changed immediately if compromise is suspected.

7. Email and Internet Use

7.1 Parish council email and internet access must be used responsibly and primarily for council business.

7.2 Users must not:

- share passwords;
- open suspicious links or attachments; or
- access unlawful or inappropriate content.

7.3 Emails containing personal or sensitive data must be handled with care.

8. Data Protection

8.1 All users must comply with data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

8.2 Personal data must:

- be kept secure;
- be used only for legitimate council purposes; and
- not be shared without proper authority.

8.3 Any suspected data breach must be reported immediately to the Chair.

9. Remote Working

9.1 When working remotely, users must:

- ensure screens cannot be overlooked;
- use secure Wi-Fi connections;
- log out of systems when finished; and
- keep devices and documents secure at all times.

9.2 Council equipment or papers must not be left unattended in public places or vehicles.

10. Social Media (Refer to Social Media Policy)

10.1 Councillors and the employee should be mindful that online activity may be associated with the Council.

10.2 They must:

- not post confidential or sensitive council information;
- not make comments that could damage the council's reputation; and
- comply with the Members' Code of Conduct and the Nolan Principles.

10.3 Only authorised persons may post on official council social media accounts.

11. Monitoring

11.1 The parish council reserves the right to monitor the use of its IT systems where necessary and proportionate, in line with data protection legislation.

12. Misuse

12.1 Misuse of council IT systems or information may result in appropriate action being taken as guided by the Disciplinary policy.

13. Review and Adoption

13.1 This policy will be reviewed periodically and updated to reflect changes in legislation, technology, or guidance issued by NALC, SLCC, or the NCSC.

Signed Chair: _____

11th May 2026