Carnforth Town Council – IT Policy

1. Purpose

This policy sets out the principles and procedures for the use of information technology (IT) systems, devices, and data within Carnforth Town Council. It aims to ensure the secure, efficient, and responsible use of IT resources to support the Council's operations and services.

2. Scope

This policy applies to all employees, councillors, contractors, and volunteers who use or have access to the Council's IT systems, including hardware, software, internet, email, and data storage.

3. Responsibilities

Town Clerk: Acts as the IT lead, responsible for overseeing IT systems and ensuring compliance with this policy.

Users: Must use IT resources responsibly, securely, and in accordance with this policy.

4. Acceptable Use

IT systems must be used for Council-related business only.

Personal use of Council IT equipment is discouraged and must not interfere with work duties or compromise security.

Users must not install unauthorised software or connect unauthorised devices to Council systems.

5. Data Protection and Confidentiality

All users must comply with the GDPR and Data Protection Act 2018.

Sensitive or personal data must be stored securely and only accessed by authorised individuals.

Data must not be shared externally without appropriate authorisation.

6. Email and Internet Use

Email accounts provided by the Council must be used for official correspondence.

Users must not use Council email or internet access for illegal, offensive, or inappropriate activities.

Phishing emails or suspicious links must be reported immediately.

7. Passwords and Access Control

Passwords must be strong, kept confidential, and changed regularly.

Users must not share login credentials.

Access to systems and data must be based on role and necessity.

8. Equipment and Software

All IT equipment remains the property of Carnforth Town Council.

Only licensed and approved software may be installed.

Equipment must be returned when a user leaves the Council or no longer requires access.

9. Security and Backup

Anti-virus and firewall software must be active and up to date.

Regular backups of critical data must be maintained.

Users must report any suspected security breaches or data loss immediately.

10. Remote Working

Remote access to Council systems must be secure and authorised.

Devices used for remote work must have appropriate security measures in place.

11. Policy Review

This policy will be reviewed annually or in response to significant changes in legislation, technology, or Council operations.

Adopted by Carnforth Town Council on: [Insert Date]

Next Review Date: [Insert Date]