COLEHILL TOWN COUNCIL

IT POLICY – ADOPTED 9th December 2025

1. Introduction

1.1 Colehill Town Council ("the Council") recognises the importance of computer systems and email in supporting its business, operations, and communications, and the need to safeguard the Council's digital data and assets.

1.2 This policy sets out expectations for the responsible use of IT and provides guidance to help Councillors and employees use systems safely and securely.

2. Scope

2.1 This policy applies to all individuals who use the computer systems and email provided by the Council, regardless of their working pattern or location, including those who are home based or office-based, flexible or part-time, Councillors or employees.

2.2 Councillor's personal computers are out of scope of this policy, see section 11 below for further advice and guidance.

3. Cyber security responsibilities

3.1 Responsibility for the administration of the Council's IT systems, has been delegated to the Clerk, either directly or through an authorised IT provider. The Council remains ultimately accountable for compliance with this policy.

3.2 The Council aims to manage its IT systems in accordance with the 2025 Practitioners' Guide.

4. Acceptable use of IT equipment

4.1 Council IT equipment is to be used for official Council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities, complies with the Councils Acceptable Usage Policy CPC Acceptable Use Policy or violate any part of this policy. All users must adhere to ethical standards and respect copyright and Intellectual Property Rights.

5. Computer and software usage

5.1 Employees who need to use IT in their role will be provided with authorised, licensed computer equipment, software, and applications for work-related tasks.

5.2 All equipment issued will be listed on the asset register.

5.3 All computers and other devices supplied should be treated with good care at all times to avoid loss or damage that would have a financial impact on the Council.

5.4 The installation of any unlicensed software on Council devices is strictly prohibited.

5.5 All devices, including computers, laptops, and mobile phones must be kept up to date with security software. Automatic updates should be enabled where possible, or devices should be updated on a regular schedule.

5.6 Regular data backups of Council devices should be performed to allow for a prompt recovery of essential services following a cyber security incident.

6. Email communication

6.1 All Councillors and employees who need to use email as part of their role will normally be given their own email address and account on a domain owned by the Council.

6.2 Email accounts provided by the Council are for Council and Council related communication only. Emails should be professional and respectful in tone, and not contain material that could bring the Council into disrepute. Councillors must use their Council-provided email account for official business so that Council data remains secure and under Council control. Using personal email should be limited and only when absolutely necessary.

6.3 To reduce the risk of phishing and other email threats, users should take the following precautions:

- Be cautious of unexpected or unusual emails, particularly those asking you to click a link, open an attachment, or provide information.
- Check the sender’s email address carefully, not just the display name. Fraudulent emails often imitate familiar names but use incorrect or unusual addresses.
- If an email seems suspicious, do not reply, click links, or open attachments. Forward suspicious emails to report@phishing.gov.uk.
- Do not trust urgent or threatening wording, as this is often a sign of phishing attempts.

7. Password and Account Security

7.1 All user accounts must be protected by strong, secure passwords.

7.2 Additional requirements:
(a) Default passwords should be changed immediately upon installation or setup.
(b) Passwords are personal and must not be shared under any circumstances.
(c) Passwords must not be stored in plain text or written down in insecure locations.
(d) Passwords must be changed immediately if compromised.

8. Monitoring

8.1 The Council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and employees or Councillors are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws.

9. Training and Awareness

9.1 The Clerk will advise Councillors and staff of relevant training resources and opportunities, including those offered through the county association.

9.2 Councillors are strongly encouraged to complete basic cyber security awareness training and report completion of any relevant training to the Clerk.

10. Compliance

10.1 The Council expects its computer systems and email to be used responsibly; inappropriate and unauthorised use will be taken seriously.

10.2 Any misuse of Council IT resources by employees may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

10.3 Compliance with this policy is part of a Councillor's responsibility.

11. Guidance for Councillors using their own Equipment

11.1 Councillors who use their own personal equipment for council emails or any other council related activity bear the responsibility for ensuring the device is free from viruses and that all software is licensed.

11.2 Councillors are strongly advised to follow the guidance in section 7 above for setting strong passwords. If they are in an environment where a computer is used by more than one person, then they should use individual logins to keep the Councillor‘s information, email and "business" separate from other users.

11.3 Any loss or security threat on personal equipment should be advised to the Clerk.

Version History

Date	Summary of Changes
9/12/25	New Policy

As this is a new policy it will be reviewed again after six months in June 2026.