



COLEHILL TOWN COUNCIL

IT POLICY – ADOPTED 14th July 2026

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 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 Any Council devices being used by councillors will be returned to the Town Clerk whenever requested, and at least on an annual basis, to check that no unauthorised software has been installed, and that there is no evidence of inappropriate use, as per the Acceptable Use Policy.
- 5.6 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.
- 5.7 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. Confidential Data

- 8.1 Confidential data such as personal information and any other highly sensitive data should not in normal circumstances be saved by councillors on their own devices, but only held by Council staff on council owned equipment. If, by exception, the Town Clerk needs to share any confidential data then it will be password protected, with the password sent by separate email. Councillors must delete confidential data when requested to do by the Town Clerk.

9. Monitoring

- 9.1 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.

10. Training and Awareness

- 10.1 The Clerk will advise Councillors and staff of relevant training resources and opportunities, including those offered through the county association.
- 10.2 Councillors are strongly encouraged to complete basic cyber security awareness training and report completion of any relevant training to the Clerk.

11. Compliance

- 11.1 The Council expects its computer systems and email to be used responsibly; inappropriate and unauthorised use will be taken seriously.
- 11.2 Any misuse of Council IT resources by employees may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.
- 11.3 Compliance with this policy is part of a Councillor's responsibility.

12. Use of Own Devices by Councillors

- 12.1 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 and kept up to date, with all relevant operating system and application security updates and patches applied promptly to protect against known vulnerabilities.
- 12.2 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, ensuring council related data cannot be viewed or retrieved by family or friends who may use the device.

- 12.3 In cases of legal proceedings against the Council, the Council may need to temporarily take possession of a device, whether Council-owned or personal to retrieve relevant data.
- 12.4 Councillors must inform the Town Clerk if a device used for Council business is lost/stolen or inappropriately assessed with any risk of access to Council data.
- 12.5 Council data should not be copied to or from a Councillor's device using removable media (including USB drives, external hard drives, CDs, DVDs or similar devices) without express permission from the Town Clerk. Following any such transfer, the media must be securely wiped of all council data.
- 12.6 Any Council data held by Councillors on their own devices must be removed when no longer required for Council business or if the Councillor resigns.
- 12.7 The Council will make reasonable efforts to provide guidance and support where appropriate, however responsibility for the security, maintenance, and operation of personal devices remains with the individual Councillor. Any costs incurred in relation to the use, repair, replacement, or recovery of personal devices or data are the responsibility of the Councillor.

Version History

Date	Summary of Changes
9/12/25	New Policy
14/7/26	Adding requirements to check council devices annually, to protect confidential data, and to strengthen requirements for councillors using their own devices.

This Policy will be reviewed annually, next review due July 2027.