

Camborne Town Council

ICT Acceptable Use Policy

1. Policy Overview

Camborne Town Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its businesses, operations and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers and contractors.

2. Scope

This policy applies to all individuals who use Camborne Town Council's IT resources, including computers, networks, software, devices, data and email accounts.

All council owned or leased ICT such as:

- PCs
- Laptops
- Notebooks
- Smartphones
- Software
- Services
- Storage media
- Network resources

3. General Responsibilities

You must:

- Protect your username, password, and security token against misuse
 - Operate a clear screen policy when you leave your computer unattended.
This can be done by, for example, "locking" the computer by:
 - pressing the ctrl, alt and delete keys simultaneously
 - clicking the "Lock Computer" button on the screen
 - Prevent inadvertent disclosure of information and avoid being overlooked when working
 - Protect hard copy material, portable devices, and removable media at all times. You must ensure they remain accounted for. When not in use you must secure them under lock and key
 - Ensure all removable media and portable ICT are encrypted
-

- Securely destroy printed material and removable media when no longer required
- Ensure personal use of the internet is reasonable, proportionate, and occasional
- Only access or attempt to access ICT you have been authorised to access
- Only access or attempt to access information for official council purposes aligned with your role. This must be on a need-to-know basis
- Connect council ICT such as desktops and laptops to the council's network continuously for at least six hours per month to receive security updates. This can be directly or remotely via AOPVN. You must ensure devices remain connected until updates have been received and applied, for example Windows updates

4. Acceptable Use

You must not:

- Use the username and password of another person
- Share your own username and password with another person
- Misuse, bypass, or subvert the configuration or security settings of any ICT
- Introduce unauthorised software, hardware, removable media, or files
- Process or access inappropriate material, including:
 - a) racist
 - b) sexist
 - c) defamatory
 - d) offensive
 - e) obscene
 - f) illegal
- Carry out illegal, fraudulent, or malicious activity
- Use ICT to carry out or support business which is unrelated to the council
- Break copyright or carry out any activity that negatively impacts intellectual property rights

5. Email

You must:

- Only transmit emails from your own authorised account
- Use file share software when sending sensitive data external to the council, for example personal data
- Check that the recipients of e-mail are correct to avoid accidental release to unintended recipients. Care must be taken when using auto complete to avoid the inclusion of an unintended email address
- Consider password protecting email attachments to mitigate the risk of sending an email to an incorrect recipient

- Use the blind carbon copy (BCC) feature when sending an email to more than one recipient and it is necessary to protect email addresses. An example of this could be when sending an external email to multiple members of the public or multiple suppliers

You must not:

- Auto-forward council email (@camborne-tc.gov.uk) to a non-CTC corporate email address as security of alternative email addresses cannot be assured
- Use personally owned email accounts to conduct official business or to transmit or receive council information

Malicious email:

- Do not open an attachment, click on any link, or respond to an email unless you are confident the email is legitimate
- Only release quarantined email if you are confident it is legitimate
- Do not forward a suspicious email unless instructed to do so by the Service Desk
- If in doubt about an email or if you think you have received a malicious email, such as a phishing email, or an email containing malicious software, report it to the Service Desk by email to support@itecgroup.co.uk immediately

Personal use of corporate email shall be:

- Reasonable
- Proportionate
- Occasional

It must not interfere with the performance of your role or the performance of the system.

6. Delegate Access

Delegate access to email accounts must only be provided following a clear business need. This must be authorised by the email account owner, or, in their absence, an appropriate member of the Senior Management Team.

When provided with delegate access the person accessing emails must take reasonable precautions to avoid opening private emails. If it becomes readily apparent that an email is of a personal nature the reader must:

- Not open it
- Stop immediately if the email has been opened

7. Passwords

Self-generated passwords must not be easily guessable for example 'letmein123', 'Password1'. They should not consist of keyboard patterns or sequential numbers for example qwerty, 12345. Passwords need to have a minimum of 12 characters with at least one special character eg ?\$%.

You must protect passwords from unauthorised disclosure.

You must not record passwords unless it is done so securely, and you are the only one who can access it.

You must not use the same password across different accounts (work and private) and, or applications.

Passwords must be changed every 60 days. It is the responsibility of each user to ensure that this is done.

Password resets- should you need a password reset email support@itecgroup.co.uk

8. New Accounts/Leavers/Changes

New users must be set up by ITEC via the Town Clerk, Deputy Clerk or Responsible Finance Officer, reusing old accounts if possible.

Oversight of all accounts will be held by ITEC but also the RFO who is the internal manager or ICT services.

Leavers - Appropriate member of SMT to advise, (copying in the RFO) ITEC of the leaver and advise them on the future of that account. Eg Closure/re-use.

Changes in role-Should a role change necessitate a need for a change of account privileges this must be requested by a member of SMT by emailing support@itecgroup.co.uk and copying in the Deputy or RFO for information.

9. Remote or Mobile Working

You must take additional care when working outside of official premises. You must apply appropriate and reasonable safeguards to manage the increased likelihood of loss or compromise.

You must only remove ICT, removable media, and hard copy information from official premises when there is a clear business need.

You must only store encrypted ICT in an unoccupied vehicle if it is secured out of sight in the locked boot. This is only if more reasonable, secure options are unavailable.

You must not store passwords and security tokens with ICT at any time.

You must not leave unencrypted ICT, removable media, and hard copy information, in an unoccupied vehicle at any time.

You must never store ICT, removable media, and hard copy information in a vehicle

overnight.

10. Reporting Security Incidents

You must report all security incidents, including near misses and suspected security incidents, in accordance with our security incident policy.

You must report all security incidents involving ICT to: the service desk by email to support@itecgroup.co.uk

What is a security incident?

A security incident is defined as any fact or event that results in the compromise, misuse, or loss of our:

- Information
- ICT services
- Assets
- A security incident can impact the confidentiality, integrity, and, or availability of information.

Examples of security incidents include:

- The loss or theft of information
- Unauthorised disclosure of, or access to, information
- Loss or theft of ICT, media, or devices
- Physical security breaches
- Deliberate or accidental breach of security policy
- Insecure disposal of information or ICT assets
- Malicious software infection
- Denial-of-service attack
- Website defacement
- Social engineering, for example a bogus contractor attempting to use a system

Near misses, suspected incidents, and security weaknesses

You must report near misses and suspected incidents in line with this policy.

A near miss is defined as:

- Any fact or event that has happened, or may have happened, but no compromise occurred.

A suspected incident is defined as:

- A situation where initial information is sparse, and it may be uncertain

whether an actual incident has taken place. A compromise of confidentiality, integrity and, or availability is nevertheless suspected.

You must report any observed or suspected information security weakness in systems, processes, or services in line with this policy. Weaknesses must not be proved or tested by unauthorised persons as this may be construed as misuse.

Actions on identifying a security incident

Remedial action must be taken as soon as possible to contain and rectify the security incident. Action must be taken to minimise the impact of a security incident and to prevent it from worsening.

You must report all security incidents involving personal data as soon as possible to ensure we meet our legal obligations regarding personal data breaches.

Personal data breaches

Security incidents involving personal data, referred to as personal data breaches, attract several reporting obligations set out in data protection legislation.

A personal data breach which is likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office (ICO) no later than 72 hours from the point we become aware of the breach.

A personal data breach which is likely to result in a high risk to the rights and freedoms of individuals must be reported to the impacted individuals without undue delay.

Whether or not a breach meets either of these thresholds will be determined on a case-by-case basis as part of the security incident investigation process.

Reporting

We will consider all security incidents for onward reporting to internal and external stakeholders. We will also consider notification to individuals affected by a breach.

Reporting requirements will be dictated by:

- The severity of the security incident
- Any statutory or contractual requirements

Examples include:

- Line managers
- Information asset owners
- Caldicott Guardians
- Senior Information Risk Owner
- Sharing partners and suppliers

- Law enforcement agencies
- The Information Commissioner's Office (ICO)
- Members of the public
- National Cyber Security Centre

11. Training and Awareness

Camborne Town Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

12. Compliance and Consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

13. Policy Review

This policy will be reviewed annually to ensure its relevance and effectiveness.

Updates may be made to address emerging technology trends and security measures.

It must be communicated to all relevant stakeholders and incorporated into Camborne Town Council's operational practices.

14. Supporting Policies and Procedures

- *Camborne Town Council Staff Handbook- Email and Internet Policy*
- *Councillor Tablet Loan Agreement*
- *Camborne Town Council Data Protection Policy*
- *Camborne Town Council Freedom of Information Policy*
- *Camborne Town Council Privacy Notice*

POLICY DATED: 12th March 2026

REVIEW DATE: 1 years after date of policy

Version number	Date	Description of changes	Author/Responsible party
1	12.06.2026	Adopted/Reviewed by Camborne Town Council Resolution number	Deputy Town Clerk