Chipping Campden Town Council
Computer and Information Security Policy
A Guide for Councillors and Employees

Information Security

Chipping Campden Town Council (The Council) provides computers and applications that provide access to the Internet and Email. Their use carries with it a responsibility to use these facilities in a safe and secure manner. In doing so you are acting in a way that is vital to the health of the council.

As an aid to understanding your role in security, this policy document provides general instruction on protecting information and assets and outlines the responsibilities that are required.

This information is provided to protect you and the council; you must read, understand and follow the principles that follow.

If you have any questions or needs additional guidance you should contact the Town Clerk.

Computer Use
All computers provided by The Council are the property of The Council and shall only used with the council's best interests in mind. As such, they shall **not** be used for the access or distribution of material considered to be obscene or for private and personal purposes.

You are responsible for the security and proper use of your computer hardware, software and data. It is important to understand security concepts and be aware of the policies, procedures, rules and guidelines concerning their use and security. These are described in this document.

Do

- Log off your PC when it is not in use
- Where available use a password protected screen saver.
- Back up all data on your computer at least once a week and keep the back up discs / memory stick in a safe and secure place in your home.

Don't

- Use equipment provided by The Council for any other purpose than for The Council business purposes.

- Bring in any floppy discs, USB keys or any other storage media unless authorised to do so.

- Dismantle, change settings or add any hardware or software to any equipment. Changes to any Council equipment must be carried out by the Computer Maintenance Provider.

- Remove equipment offsite without the proper authorisation.

- Remove any original, or copies of, data without the proper authorisation, Except the weekly back up discs / memory stick which is to be kept in a secure place off-site for security purposes.

- Remove any original, or copies of, documentation without the proper authorisation.

- Use or connect modems. Where there is business need to use a modem, authorisation must be obtained from the Town Clerk.

Secure Passwords
Your password acts as a personal key and provides access to computer systems and applications.

Don't share your password with anybody

If you need any guidance or feel that your password is being used by others, immediately contact the Town Clerk who will advise you what to do next.

Internet and Email Use

When using the internet and email you must **not** violate any law, interfere with network users, services or equipment, or harass other users. Failure to comply with these usage instructions could lead to disciplinary and/or legal action.

You must **not** email confidential or potentially sensitive information unless you have been given explicit authority to do so, and the appropriate level of security protection is used. It is your responsibility to determine the confidentiality of each email message you send. Assume that any message or information sent using the Internet is available to the public.

As a user of The Council's Internet and Email services you **must not** access, view, download, save, solicit, send or provide access to material related to or including:

- Offensive content of any kind, including pornographic material
- Promoting or supporting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion or disability.
- Threatening or violent behaviour
- Illegal activities
- Personal commercial activities
- Games or other entertainment software or material
- Gambling
- Personal or financial gain

- Abuse copyright laws
- Sending business-sensitive information over the internet without the appropriate permission and security protection
- Reveal data to The Council's customers, suppliers, clients, third party companies or members of the public without authorisation
- Misrepresent yourself and/or The Council
- Material that brings The Council into disrepute

Where possible you should **not** open email that is of a questionable nature, such as an email with an unusual attachment, a message from an unusual source, or unexpected email, as these are all signs that the email could potentially have hazardous or dangerous content or attachments. Where possible simply delete the message without opening it. When opening unfamiliar attachments, macros should be disabled if prompted. If you receive email that appears questionable from someone you know, contact him or her and confirm they sent the email and that the content is harmless.

Do

- Be careful when addressing email – know who you are sending to
- Remember that the recipient's culture, language and humour may have different points of reference than your own
- Apply common sense before assuming a message is valid (mail and news can be forged).

Don't

- Send chain letters via electronic mail
- Pass on, forward, cc any joke email internally or externally
- Include photographs or other graphics, or software or executable files as email content or attachments unless they are for a business purpose. The sending of such material causes a large amount of unnecessary load on the systems and can slow down the system access for business critical work.
- Transmit, or otherwise distribute proprietary information, data, trade secrets or other confidential information belonging to The Council, partners or associates unless expressly authorised to do so and the appropriate level of security protection has been applied.

Virus Protection

Anti-virus software is installed on all desktops and laptops. You should make every attempt to limit the exposure of computers to viruses and other malicious programs. It is the responsibility of all The Council staff to take responsible steps to prevent virus outbreaks. It is critically important that each person follows the procedures below to do their part:

Don't

- Open suspicious email attachments, even from co-workers.
- Open an email attachment from an unknown or suspicious source
- Download software from the internet.

If you suspect your PC has been infected by a computer virus, immediately contact the Town Clerk who will give advice on what to do next.

Storage Devices
Permission for the connection of any portable storage device to The Council equipment must be sought. This includes but is not limited to ipods, USB keys/sticks, pen drives, data vaults, MP3/media players, flashcards and PDAs.

Software
Installation of any software **must** be officially approved before it can be loaded onto Council equipment. The Computer Maintenance Provider **must** carry out the installation / loading of any software on to Council systems and equipment.

Security Breaches
There are many reasons why The Council has put these rules in place, for example sharing video access across our systems or downloading large amounts of data from the Internet has a substantial impact on the performance of the network, but primarily these rules are in place in an effort to protect The Council's employees, customers and data.

The Town Clerk has authorisation to remove back up discs / memory sticks and store in a safe and secure place at the Clerk's residence.

If you detect, witness or have information of an actual or possible breach of security, please contact the Town Clerk.

Any information will be dealt with in the strictest confidence.