Acceptable Use Policy

Full Council Approved:	3 June 2026
Last Reviewed:	June 2026
Due for next Review:	June 2029

1. Purpose

The purpose of this policy is to provide all our employees, contractors, temporary employees and third parties that are granted access to Council information assets (devices), the rules relating to the acceptable use of those assets (devices) under their control.

2. Scope

This policy applies to every individual who uses Council information assets (devices) and sets out what the Council consider to be the acceptable use of those assets.

3. Responsibilities

All employees as well as contractors, temporary employees and third parties that are granted access to Council information are required to comply with this policy.

4. Acceptable Use

All information assets, including both digital and non-digital assets are Fleet Town Council's property and, as such shall be used only for the purpose of conducting the Council's business activities and in compliance with our other information security policies.

Information assets (devices) shall only be used by authorised individuals and must not be used for any illegal purposes. Users shall report any loss and/or damage of information assets to the Executive Officer.

Fleet Town Council reserves the right to monitor the use of information assets (devices) for, as a minimum, the following purposes:

- Compliance with Council information security policies
- Compliance with legal, regulatory, and contractual requirements
- Any other purpose that the Council deems appropriate

5. General Use and Ownership

Users must be aware that the data they create on the Council's systems remains the property of Fleet Town Council. Any information transmitted over the networks

that has not been specifically identified as the property of other parties is by default treated as belonging to Fleet Town Council.

Unauthorised access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of any information is strictly prohibited. Therefore, it is recommended that any information that users consider sensitive or vulnerable be encrypted with a password.

For security and network maintenance purposes, authorised individuals within the Council, or authorised third party (i.e. Cloudy IT or other IT support supplier) may monitor equipment, systems, and network traffic at any time. Fleet Town Council reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Access to Internet and email may be restricted if the bandwidth does not support the volume, or in case of misuse.

6. Security and Proprietary Information

Authorised users are responsible for the security of their passwords and accounts. All Personal Computers (PC), laptops and workstations must be secured with passcode-protected screensavers with the automatic activation feature set, or by logging-off when unattended. Details on passwords can be found in the Password Policy.

Postings by users from Council email address to newsgroups must include a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Council unless posting is during business activities.

Users are required to use extreme caution when opening e-mail attachments received from unknown senders, which may contain malicious content and/or attachments.

7. Unacceptable Use

The following activities are, in general, prohibited, however, users may be exempt from these restrictions during their legitimate operational responsibilities such as systems administration staff, needing to disable the network access of a host, if that host is disrupting production services.

Under no circumstances is any user authorised to engage in any activity that is illegal under local, or international law while using Council owned resources. The list below is by no means exhaustive, but attempts to provide a framework for activities, which fall into the categories of unacceptable/acceptable use.

Systems and Network Activities

- Installation or distribution of "pirated" or other software products that are not appropriately licensed.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any

copyrighted software for which the Council, or the end user, does not have an active license is strictly prohibited.

- Revealing account passcodes to other users or allowing use of individual accounts by others. This includes family and other household members when work is being done at home. Users are accountable for all the activities that carried out in their respective login.
- Using a Council computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties.
- Providing information about or lists of the Council's users/customers to external parties.

Email and Communication Activities

- Sending unsolicited email messages, including "junk mail" or other advertising material to individuals who did not specifically request such material.
- Any form of harassment via email or telephone, whether through language, frequency, or size of messages
- Unauthorised use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or other such schemes of any type.
- Use of unsolicited email originating from the Council's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the business or connected via the Council's network.
- Council e-mail facilities may not be used for sending defamatory e-mails, or using e-mail for harassment, unauthorised purchases, or for publishing views and opinions, defamatory or otherwise about the Council's employees, workers, suppliers, partners, or customers.
- Outgoing e-mail attachments must be appropriately assessed to ensure if protection using cryptographic controls is required.
- Users must not open incoming e-mail attachments that originate with unknown third parties or that, even if they appear to have been sent by a known party, were not expected. These attachments may contain malicious content. Any such e-mails must be reported to the IT Helpdesk (Cloudy IT) immediately. On no account should they be forwarded or copied to anyone, whether inside or outside the network.
- Viruses and hoax virus messages: users are required to report any third-party e-mail messages they receive about viruses to the Executive Officer immediately. On no account should it be forwarded, or copied on, to anyone, whether inside or outside the network
- Users are prohibited from using Council e-mail facilities for forwarding chain letters or impersonating other people. Additionally, Council e-mail addresses are not to be left on any websites other than for legitimate and necessary business purposes.

- Users are required to limit the use of group e-mail addresses, to limit copying to unnecessary recipients, to restrict use of the 'reply to all' function and restrict the use of the blind copying feature.
- Employees are required to delete non-essential e-mail messages as soon as possible and, on a regular basis, to clear e-mail boxes of correspondence that is no longer required.
- Council e-mails may not be used to purchase anything on behalf of the Council without specific prior authorisation and then only in accordance with the Council's current policies regarding purchasing and cryptographic controls.
- Council e-mail addresses may not be used for personal purchases or any other personal transactions.
- Employees are prohibited from setting up automatic forwarding of e-mails to external addresses or of copying e-mails to addresses outside the Council, unless there is a legitimate business purpose for doing so.

Internet Usage

- Council User Identifications (ID), websites and e-mail accounts may only be used for council sanctioned communications.
- Downloads from the internet must be screened for viruses before accessing.
- Users must not place any of the Council's material in a publicly accessible internet site without prior approval.
- The Council reserves the right to examine the internet access information of any user. Use of internet/e-mail/instant messaging may be subject to monitoring for reasons of security and/or network management, and users may have their usage of these resources subjected to limitations.
- Personal use of internet is permitted so long as it does not adversely affect business activities.
- Users connecting to the council's network via Virtual Private Network (VPN), will be permitted to do so, only with specific approval from the Executive Officer.
- Users must inform the Executive Officer of any security breach that they know of or become aware of.
- The Council is not responsible for material viewed or downloaded by users from the internet. Users are cautioned that some webpages may include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with the material while using the internet. Even innocuous search requests may lead to sites with highly offensive contents. Users accessing the internet do so at their own risk. Should any illegal activities be found, such as breaches, theft, or hacking. The Council will hand the personnel information details to the appropriate law enforcement agencies.
- Users may not download software from the internet, execute or accept any software programs or other code from the internet unless it is in accordance with policies and procedures.
- Users will not seek to avoid and will uphold the Council's anti-malware policy and procedure.
- Users will not intentionally interfere in the normal operation of the network or take any steps that substantially hinder others in their use of the network. Users will not examine, change, or use another person's files or any other information assets for which they do not have explicit permission.

- Users will not conduct any other inappropriate activity as identified from time to time by the council and will not waste time or resources on non-council business. This includes downloading bandwidth intensive content, such as streaming videos and music files and sharing digital photographs.

9. Enforcement

Users shall abide to existing information security policies and procedures. Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract or agreement.

10. Related Documents

- Access Control Procedure
- Anti-Malware Policy
- Information Security Awareness Policy
- Password Policy