



TOWN OF CASCO

EMPLOYEE TECHNOLOGY AND SOCIAL MEDIA POLICY

Section 1. Purpose:

This policy applies to all Town employees (referred to as either “employees” or “users”). The purpose of this policy is to define the requirements and responsibilities that all employees connecting to or using the Internet through the Town of Casco’s own internet network (the “Town Network”) must follow. This policy provides awareness and notification of what we deem to be acceptable and unacceptable use of the Town Network in order to ensure that the Town Network is properly used to avoid both distractions in the work environment, as well as harm to the Town’s reputation or financial well-being. This policy further articulates the Town’s expectations related to employee use of social media.

Section 2. Authorized and Unauthorized Usage:

Personal or incidental use of the Town Network is authorized for limited purposes and will be subject to the following guidelines:

- Use must not constitute a conflict of interest. For example, personal business or use for personal gain constitutes a conflict of interest.
- Use is on personal time (hours not charged to the Town) and must not interfere with our business or normal work activities, and must not adversely impact performance of the employee, surrounding employees, the organization, or business functions.
- Illegal, obscene, pornographic, or offensive material must not be accessed, viewed, downloaded, or sent.
- Any access that could result in a significant incremental cost, including, but not limited to, noticeable additional e-mail traffic and large non-business related file transfers, is not permitted.
- Use must not involve any illegal or unethical activity (e.g. gambling, use of pirated software, movies, games, or illegal hacking tools).
- Transmitting or sending sensitive or proprietary information, including software applications or personal information, to unauthorized persons or organizations is prohibited. Authorization for any transmission of personally-identifying information (“PII”) must be approved by a supervisor prior to transmission and done using authorized protocols (e.g. encryption, VPN, SSL).
- Downloading or sending unapproved software, computer viruses, malicious code, or any unauthorized attempts to access another person’s data or Town’s intranet are prohibited.
- The addition of any hardware that would allow additional access to the Internet is prohibited.
- Users may not download software from any outside systems without permission from the Information Technology Department (“Information Technology”). Users should not use any externally-provided software without first getting approval from Information Technology. Users should not download unapproved or unauthorized software from the Internet. Users are responsible for determining the sensitivity and need for further encryption to secure Town Sensitive Information or PII prior to posting, transmitting, or sending it via the Internet. If unsure, the user is responsible for contacting Information Security for assistance.

- Users are prohibited from using the Town website or web servers for posting non-business related data or for the illegal distribution of data, such as software, games, movies, code or other inappropriate data.

Section 3. Privacy & Monitoring:

By using the Internet access provided by the Town, users must agree to this policy and acknowledge that record of Internet access, such as sites visited, images reviewed, and e-mail sent, may be recorded and monitored by the Town at any time with no expectation of privacy and that:

- Encrypted technology that meets the Town's requirements will be employed.
- The Town owns the rights to all data and files in our computers, network, or other information systems, subject to applicable laws. Users may not access networks, servers, drives, folders, or files to which the user has not been granted authorization. Users may not destroy, delete, erase, or conceal files or other data, or otherwise make files or data unavailable or inaccessible. In addition, users may not access another employee's computer, computer files, or e-mail without authorization from their supervisor.
- The Town licenses the use of certain commercial software application programs from third parties for business purposes. Third parties retain the ownership and distribution rights to this software. Users may not use or distribute licensed software.
- E-mail messages and other electronic correspondence sent and received using the Town's equipment or Internet access provided by the Town are not private and are subject to viewing, downloading, inspection, release, and archiving by the Town. The Town reserves the right to inspect files stored in private areas of the Town Network or on individual computers or storage media in order to ensure compliance with our policies and state and federal laws. The Town additionally reserves the right to monitor e-mail messages, and any other electronic correspondence that occurs on the Town Network or with Town equipment.
- The Town may use software that allows the Town to monitor messages, files, or other information that is entered into, received by, sent, or viewed on the Town's network. By using the Town's equipment or Internet access provided by the Town, users will consent to the monitoring of all network and information systems.

Section 4. E-Mail and Instant Message Use:

Users are prohibited from creating or sending e-mail or other electronic correspondence:

- That may be considered offensive or harassing, or that may contribute to a hostile environment;
- That contains profanity, obscenities, or derogatory remarks;
- That constitutes chain letters or spam;
- To solicit or sell products; or
- To distract, intimidate, or harass anyone, or to disrupt the workplace.

Users are instructed to demonstrate caution when opening e-mail and attachments from unknown senders in the event that these electronic communications may contain viruses, root kits, spyware or

malware that can put the Town's system and sensitive information at risk. Users are expected to follow appropriate instructions regarding the proper use of Instant Message use and measures to prevent unauthorized disclosure of Town Sensitive Information and PII if IM is used.

Section 5. Social Media:

This policy addresses social media activity by employees of the Town. The Town recognizes and appreciates that an employee has the right to utilize social media in the employee's personal capacity and that such use is afforded certain constitutional and statutory protections. This policy governs social media activity to the extent that such activity either undermines or interferes with the ability of the Town to carry out its responsibilities, which is activity that may be subject to the Town's review and corrective action.

An employee's personal use of social media outside of employment is at the employee's discretion. However, to the extent that any social media activity relates to the employee's employment, Town employees are prohibited from using social media in such a way that creates the impression that the employee is speaking on behalf of the Town. Town employees are additionally prohibited from sharing any confidential information, including Town Sensitive Information and PII, on social media, and using Town-issued e-mail addresses for any personal social media account.

Further, employees do not have an expectation of privacy in their use of social media when such use is used through any Town system or on a Town-provided device. Please see the Privacy & Monitoring Section described above.

This policy does not limit any employee rights pursuant to the Municipal Public Employees Labor Relations Law, or similar laws related to collective bargaining.

Section 6. Termination:

Former employees of the Town remain responsible for maintaining the confidentiality of Town Sensitive Information and PII the former employee may have previously had access to.

Section 7. Compliance

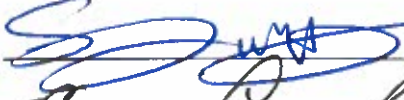

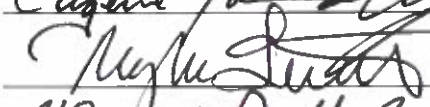
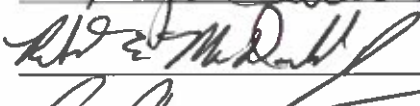

Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment. We reserve the right to advise appropriate authorities of any violation of law.

Section 8. Accountability

All employees are responsible for the secure handling, processing, transmittal, and safeguarding of Town Sensitive Information and PII.

Adopted this 11th day of July 2023.

Approved by Casco Selectboard:

	Scott Avery, Chair
	Eugene Connolly, Vice-Chair
	Mary-Vienessa Fernandes
	Robert MacDonald
	Grant Plummer