



CASTINE_{MAINE, U.S.A.}

TOWN OF CASTINE INTERNET USE POLICY

Purpose

The purpose of this policy is to define the requirements and responsibilities that all users connecting or using the Internet through the TOWN OF CASTINE (hereinafter the "Town") Network must follow. This policy provides awareness and notification of what the Town deems to be acceptable and unacceptable use of the Town Network.

It is necessary to make sure that the Town Network is properly used to avoid distractions in the work environment and harm to the Town's reputation or financial well-being. To do this, the Town relies upon several critical practices and end user behaviors.

Applicability

This policy applies to all users, including administrative consultants, employees, contractors, administrators, and third parties that have access to the Town Network. By using the Internet access provided, the user must agree to this policy and acknowledge that the Town may record and monitor records of Town's user IDs and Internet access at all times with no expectation of privacy, whether using a Town computer or using a personal laptop, but connecting through the Town network or using Town credentials.

Scope

Information assets that process data electronically in conjunction with the Internet, if used properly in conducting business related purposes, can be a valuable asset. Used correctly, the Town Network can provide a wide range of information, as well as facilitate the appropriate secure transmission of business related information efficiently.

Policy

This document provides the guidelines for establishing a culture of trust and integrity where users are committed to playing an integral part in protecting employees, consultants, contractors, partners, clients, and the Town from malicious, illegal or damaging actions, either knowingly or unknowingly. Inappropriate use exposes the Town to potential risks and vulnerabilities that might compromise important data.

Internet/intranet/extranet access is granted expressly for employees and other users for the purpose of conducting approved business purposes; computing equipment, operating systems, software, storage media, email, web browsing, FTP and network accounts are all associated with and the property of the Town.

An effective Information Security Program requires a team effort involving the participation and support of all Town employees, consultants, contractors and users who handle the Town's information and connect to the Internet via the Town Network.

Authorized and Unauthorized Usage

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

- The use must not constitute a conflict of interest. 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 the Town's business or normal work activities, and must not adversely affect performance of the employee, surrounding employees, the Town, or business functions.
- Illegal, obscene, pornographic, or offensive material must not be accessed, viewed, downloaded or sent.
- Any access that could result in significant incremental cost, such as noticeable additional electronic mail traffic, large non-business related file transfers, and the like are not permitted.
- Use must not involve any illegal or unethical activity (e.g. gambling, Warez sites containing pirated software, movies, games, or illegal hacking/cracking 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 Identifiable Information ("PII") must be approved by a supervisor prior to transmission and done using authorized protocols (e.g. encryption, VPN, SSL).
- Downloading or sending of unapproved software, computer viruses, malicious code, or any unauthorized attempts to access another person's data or the Town's intranet are prohibited.
- The addition of any hardware that would allow additional access to the Internet is prohibited.
- Users should not bring personal computers or data storage devices (such as CDs/DVDs, external hard drives, USB or flash drives, iPods, or other data storage media) to connect them to the Town's systems without permission from the Town. Personal electronic devices are subject to inspection; if a user does not wish his or her personal computer or other devices inspected, then the user should not bring those items to work.
- Users may not download software from any outside systems without permission from the Town. Users should not use any externally provided software without first getting approval from the Town. 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 the Town for assistance.
- The Town's privacy policy should be posted on all official Town websites to ensure that customers and clients are aware of the Town's desire to maintain and protect the privacy of Town data.
- Town websites or web servers are not to be used for posting non-business related data or for the illegal distribution of data, such as software, games, movies, code or other inappropriate data.

Privacy & Monitoring

By using the Internet access provided by Town, users must agree to this policy and acknowledge that records of Internet access, such as sites visited, images reviewed, and email 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 the Town's 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 electronic 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.
- Electronic mail ("email") messages sent and received using Town 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 has the right to inspect files stored in private areas of the Town Network or on individual computers or storage media in order to assure compliance with Town policies and state and federal laws. The Town may monitor electronic mail messages (including personal/private/instant messaging systems).
- 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 Network. By using Town equipment or Internet access provided by the Town, users will consent to the monitoring of all network and information systems.

Reporting of Internet Abuse

- An email account link is established to receive complaints and concerns from external non-employees pertaining to Internet activity possibly originating from the Town Network.
- Contractual documentation will specify the scope of the electronic transmissions and the services and devices required.
- Complaints to this account will be forwarded to the Town Manager.

Electronic Mail and Instant Message Use

Policies and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software.

Users are prohibited from creating or sending electronic mail:

- 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 services that are unrelated to Town business; or
- to distract, intimidate or harass anyone, or to disrupt the workplace.

Users are instructed to use caution when opening electronic mail and attachments from unknown senders because these pieces of electronic mail and attachments may contain viruses, root kits, spyware or malware that can put the Town system and sensitive information at risk.

Users will be provided appropriate instructions about the proper use of IM and measures to prevent unauthorized disclosure of Town Sensitive Information and PII if IM is used.

Termination

Even after termination of a user's relationship with the Town, users are responsible for maintaining the confidentiality of Town Sensitive Information and PII the user may have had access to previously.

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. The Town reserves the right to advise appropriate authorities of any violation of law.

Accountability

All employees, consultants, contractors, and non-employee users are responsible for the secure handling, processing, transmittal and safeguarding of Town Sensitive Information and PII. This responsibility is fulfilled by the acceptable use of the Town Network and the Internet access the Town provides.

Third parties/vendors are responsible for ensuring their use and access to the Town and its computing resources, whether on their own information assets or on Town assets, meet the Town's security protections and safeguards and that the assets are used appropriately.

The Town is responsible for ensuring that a user acknowledgement or a non-disclosure agreement has been signed by all users acknowledging this Policy before providing access to the Town's sensitive computing resources.

The Town is responsible for ensuring compliance with this Policy and the controls created to safeguard the Town Network.


ADOPTION

This policy is adopted by the Castine Board of Selectmen on the 4th day of May 2015. This policy shall remain in effect until repealed by the Board of Selectmen.


Peter F. Vogell


David G. Unger


Constantino G. Basle

Attest:  May 4, 2015
Susan M. Macomber, Town Clerk

SEAL