Town of Waldoboro

Information Technology POLICY

Contents

General Policies

1. Acceptable Use

1.1. Overview

The Town of Waldoboro's (herein also known as the Town) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Town's established culture of openness, trust and integrity. The Town is committed to protecting the Town's employees, supervisors and the Town from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet & Intranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts electronic mail (e-mail), WWW browsing, and FTP, are the property of the Town of Waldoboro, and thus subject to the *Maine Freedom of Access Law*, M.R.S.A. 1, Chapter 13, §§401 – 521 et. al. These systems are to be used for business purposes in serving the interests of the Town in the course of normal operations. Personal use of Town computers by Town employees is acceptable, during the off time of the employee, providing the employees use discretion and comply with the policies outlined in this document.

Effective security is a team effort involving the participation and support of every Town employee, at every level, who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

1.2. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at the Town, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Town.

2. General Use and Ownership

2.1. While the Town desires to provide a reasonable level of privacy, users should be aware that the data they create on the Town systems is the property of the Town. Because of the need to protect the Town's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the Town, with the exception of confidential folders on the shared network "H:/" drive (described further in section 3.1.).

2.2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for

creating guidelines concerning personal use of Internet & Intranet systems. If there is any uncertainty, employees should consult their supervisor.

2.3. The Town recommends that any information that users consider sensitive or vulnerable be placed into a password protected folder. For guidance with this process, please contact the I.T. Department.

2.4. For security and network maintenance purposes, authorized individuals within the Town may monitor equipment, systems and network traffic at any time.

2.5. The Town reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3. Security and Proprietary Information

3.1. Employees are required to store all Town data on the Town's server (the 'H:/ Drive'), or the Town's official website (www.waldoboromaine.org), so it can be backed up on a regular basis to avoid loss of data due to a workstation malfunction and for effective compliance of Maine's Right to Know Law. Folders on the H:/ drive should be classified as either confidential or not confidential, as defined by the Department Head or Town Manager. All State and federal guidelines are applicable. Examples of confidential information include but are not limited to: personnel records and documentation, HIPPA guidelines, and ongoing police investigations. Employees should take all necessary steps to prevent unauthorized access to this information. All folders on the H:/ drive have limited access per user or user group, depending on individual user needs.

3.2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Users may be required to change their password on an administration determined period of time.

3.3. Password complexity requirements: Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters. Passwords must be at least six characters in length. Passwords must contain characters from three of the following four categories:

3.3.1. English uppercase characters (A through Z).

3.3.2. English lowercase characters (a through z).

3.3.3. Base 10 digits (0 through 9).

3.3.4. Non-alphabetic characters (for example, !, $, #, %).

3.4. All PCs, laptops and workstations should be secured by logging-off (*CTRL-ALT-DEL*) or (*WINDOWS KEY-L)* when the computing device will be unattended.

3.5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Mobile computing and storage devices containing or accessing the information resources on the Town's H:\Drive must be approved by the I.T. Coordinator prior to connecting to the information systems at the Town, regardless of ownership.

3.6. Postings by employees from a Town email address to newsgroups, blogs, etc. should only be in the course of business duties.

3.7. All devices used by the employee that are connected to the Town Internet and / or Intranet, whether owned by the employee or the Town, shall be continually executing approved virus-scanning software with a current virus database.

3.8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, or known senders which the employee is not specifically expecting an attachment, which may contain viruses, e-mail bombs, Trojan horse code, or other malicious software. If you are not expecting an attachment from a known sender, call or email the sender to verify its validity.

4. Unacceptable Use

Under no circumstances is an employee of the Town authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the Town owned resources.

The lists below are not intended to be exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.1. System and Network Activities

4.1.1. Password protecting, locking, or otherwise making a file inaccessible to the I. S. Manager. Instead, please use the recommended method of placing the file into a confidential folder as described in §3.1 of this Policy.

4.1.2. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

4.1.3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, or the installation of any copyrighted software for which the Town or the end user does not have an active license is strictly prohibited.

4.1.4. Installation of software on the Town's computing devices unless a prior request and approval is obtained by the requester's department head and approved by the I.S. Manager.

4.1.5. Bypassing a computing device's anti-virus program to run a program or visit a website unless a prior request and approval is obtained by the requester's department head and approved by the I.S. Manager. Disabling the anti-virus software on a workstation is strictly forbidden with few exceptions (under these extenuating circumstances, when the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing).

4.1.6. Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.1.7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members.

4.1.8. Using a Town computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

4.1.9. Making fraudulent offers of products, items, or services originating from any Town internet or intranet account.

4.1.10. Making statements about warranty, expressed or implied, unless it is a part of normal job duties.

4.2. <u>Email and Communications Activities</u>

The following guidelines are to prevent a derogatory public image of the Town by misconception of an employee's viewpoint or political stand, and therefore prohibited. When email is transmitted from the Town, the general public will tend to view that message as an official policy statement from the Town.

4.2.1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

4.2.2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

4.2.3. Unauthorized use, or forging, of email header information.

4.2.4. 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.

4.2.5. Creating or forwarding "chain letters", "Ponzi" (fraudulent investment schemes) or other "pyramid" schemes of any type.

4.2.6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3. <u>Social Media</u>

4.3.1. Use of social media by employees, whether using the Town's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the Town's systems to engage in these activities is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the Town's policy, is not detrimental to the Town's best interests, and does not interfere with an employee's regular work duties. It is understood that some Town employment positions require interaction with social media.

4.3.2. Employees shall not engage in any activities that may harm or tarnish the image, reputation and/or goodwill of the Town and/or any of its employees. Town employees have a responsibility to help communicate accurate and timely information to the public, regardless of whether the communication is in the employee's official role or in a personal capacity. It is important for employees to remember that even some personal communication of employees may reflect on the Town, especially if employees are commenting on anything political in nature. The following guidelines apply to personal communication including social media:

4.3.2.1. Remember that what you write is public and may be for a long time. Use common sense. Refrain from posting information that you would not want your supervisors or other employees to read.

4.3.2.2. The Town expects its employees to be truthful, courteous, and respectful.

4.3.2.3. Avoid negative, sarcastic, or other comments that may damage the team atmosphere between or within Departments.

4.3.3. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when using social media or otherwise engaging in any conduct prohibited by the Town's Non-Discrimination and Anti-Harassment policy.

4.3.4. Employees may also not attribute personal statements, opinions or beliefs to the Town when engaged in these activities. If an employee is

expressing his or her beliefs and / or opinions in social media, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the Town, and may not include any items in §4.3 of this Policy. Employees assume any and all risk associated with social media.

4.3.5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the Town's logos and any other the Town intellectual property may also not be used in connection with any social media activity without explicit permission from your Department Head and the I.S. Manager.

4.4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

APPENDIX A: Definitions

Blogging - Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

Chain email or letter - Email sent to successive people. Typically, the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

Computing device - any device that is used to access a service through the internet or intranet via a wired or wireless connection.

Intranet - An intranet is a private computer network that uses Internet technologies to securely share any part of an organization's information or operational systems with its employees.

Mobile Devices - Mobile media devices include, but are not limited to: internet cell phones, PDAs, plug-ins, USB port devices, CDs, DVDs, flash drives, modems, handheld wireless devices, and any other existing or future media device.

Removable Media - Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks not provided by the Town of Waldoboro.

Spam - Unauthorized and/or unsolicited electronic mass mailings.

Town of Waldoboro network - A wired or wireless network including indoor and outdoor networks that provide connectivity to Town services.

Adopted Date: February 14, 2012
Amended: June 28, 2016

Board of Selectmen:
Town of Waldoboro, Maine

_____
Joanne C. Minzy, Chair

_____
Ronald L. Miller, Vice-chair

_____
Clinton E. Collamore

_____
Abden S. Simmons

Attest,

_____
Linda-Jean Briggs
Town Manager

_____
Katherine W. Winchenbach