



# POLICY

# 2014-04

**TO:** Town of Milton Selectboard  
**CC:** Brian Palaia, Town Manager  
**FROM:** Erik Wells, Exe. Assistant to the Town Manager / HR Coordinator  
**RE:** Policy 99-02 as Revised 12/15/14- Information Technology Use Standards  
**DATE:** December 15, 2014

**EFFECTIVE UPON ADOPTION BY THE SELECTBOARD**

**PURPOSE:** This policy (first revision September 12, 2005 and this current iteration) is now renamed to change “computer” to “information technology.” It protects and ensures the integrity of the Town of Milton’s (“Town”) data and information systems. Computers, telephones, tablets and any future telecommunication assets are the property of the Town, similar to other tangible assets. The ability of the Town to successfully serve the citizens and employees of Milton depends, in part, upon the continuing availability of computers, mobile devices, data, server space, website, social media platforms and software acquired for the purpose of conducting and administering the business of the Town. Whether online, interconnected or stand alone, these resources represent the municipal information technology system.

**SCOPE:** This policy applies to employees including full time, part time and temporary workers, independent contractors, consultants, and other workers at the Town, including all personnel associated with third parties. It also applies to volunteers elected or appointed to serve on Boards or Commissions. This policy applies to all the equipment that is owned, leased or registered by the Town. For example, computer hardware and software, internal network drives and related systems, the Town website, social media accounts, voice communication equipment, voice mail, operating systems, storage media, network accounts, email accounts and internet use information are the property of the Town. This list may not be all inclusive, and future assets should be listed in policy revisions. These systems are to be used by the Town as tools for municipal governance and administrative management in serving the interests of the public.

**GENERAL USE:** The Town information technology network is to be used for the purpose of conducting Town business. For employees, occasional, brief, and appropriate personal use of the Town computer system is permitted during a scheduled break, provided it is consistent with this policy and does not interfere with job duties or responsibilities.

All users should have no expectation of privacy regarding anything created, sent or received using the Town information technology network. The data created on Town systems remains the property of the Town. This includes documents, spreadsheets, presentations, web sites visited, etc... Due to the need to protect the Town's telecommunication and information networks, and for security and network maintenance purposes, third-party contracted service authorized personnel may monitor and need to repair equipment, systems and network configurations at times. The Town reserves the right to audit networks and systems for security and data protection purposes at any time. All files, documents, data and other electronic messages created, received or stored on the Town computer system are open to review and regulation by the Town and may be subject to the provisions of Vermont's Public Record Law.

**CONFIDENTIAL INFORMATION, ACCESS, AND SYSTEM SECURITY:**

1. Data that is confidential in nature will be properly stored on network drives and access regulated and protected by user authorization and permissions. This includes software programs used to analyze and manage this information (i.e. NEMRC). Examples of confidential information include but are not limited to: Financial, Employee personnel files and files relating to labor issues. Town Employees should take all necessary and reasonable steps to prevent unauthorized access to this information.
2. Employees should make a reasonable effort to save all necessary files on network drives to ensure the data is backed up. Data saved on user profiles and/or the local computer disk runs the risk of being lost or compromised.
  - a. Network users shall keep their passwords secure and not share with other users. The Town Manager's Office may be granted access to files saved on user profiles and local computer drives in the event of an absence of the employee when the data is needed in a time sensitive manner.
3. Employees and Selectboard Members are provided with a Town email address (ending in [@town.milton.vt.us](mailto:@town.milton.vt.us)). Board and Commission members are also provided with a Town email address (ending in [@miltonvt.org](mailto:@miltonvt.org)). All personal email should be sent from a personal email account, reasonable exceptions (i.e. communicating with family members, partners, roommates, etc... for circumstances that warrant email communication using the Town address for quick access to users is acceptable). This is discretionary for users to determine.
  - a. Remote access to Town email accounts is available through a web portal and mobile devices. If access to a Town email account is gained through a

personal device (i.e. smartphone or computer) the data transmitted via the email account is still the property of the Town. All security protocols outlined in this policy are subject to any remote access and use of a Town email account by a user.

- b. Employees shall exercise extreme caution when opening email attachments received from unknown senders, which may contain viruses or other intrusive and harmful mechanisms. A software program scans email from questionable sources and provides the user with a summary.
- c. It is recommended that employees change their password quarterly for added security.
  - i. Users who have a confidential password to access the Town's operating system should be aware that that this does not mean the computer system is for personal confidential communication, nor does it suggest that the computer system is the property of that person.
- d. Town email addresses should not be used to manage personal accounts (i.e. banking, social media, online shopping websites).
- e. Transmission of electronic messages on the Town computer system shall be treated with the same degree of propriety, professionalism, and confidentiality as written correspondence.
- f. Email messages that are intended to be temporary, non-substantive communications may be routinely discarded. However, users must recognize that emails sent, received, or stored on the Town computer system are subject to Vermont's Public Records Law and may be covered by the State of Vermont's retention schedule for municipal records.

**PROCEDURE:** Town technology shall not be used in any manner prohibited by law or disallowed by licenses, contracts, Town or departmental regulations. All employees share responsibility for protecting these files from abuse. The following list of examples of abuse is by no means exhaustive, but it is an attempt to provide a framework for activities which fall into the category of unacceptable use:

- Communication that in any way may be construed by others as disruptive, offensive, abusive, discriminatory, harassing or threatening;
- Unauthorized use of computer or related equipment;
- Attempting to access files other than one's own without permission;
- Interference with any computer system or another's use of any computer system;
- Using technology assets to send or receive messages that may indicate or suggest pornography, unethical or illegal solicitation, racism, sexism or inappropriate language;
- Visiting known pornographic internet sites or returning to pornographic internet sites once the context of the site is known;

- Using a Town technology asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws;
- Making fraudulent offers of products, items and services provided originating from a Town email account;
- Theft, use and distribution of illegally copied software;
- Intentionally damaging software, files or equipment;
- Creating or using software or email designed to destroy data and/or disrupt services;
- Unauthorized access to, or manipulation of service, router, server, hubs and other network resources;
- Modifying, changing or otherwise interfering with the physical and logical configuration of computer hardware and software without authorization;
- More than minimal use of technology, software and internet access for personal business;
- Using someone else's identify (user identification ID, name);
- Intentionally or unlawfully misrepresenting your identify or affiliation in electronic messaging communications;
- Distributing copyrighted materials by electronic messaging without consent from the copyright owner. Failure to obtain consent may violate federal copyright infringement laws and could subject the individual to civil liability or criminal prosecution;
- Downloading information of programs from the internet without following protocols for virus protection;
- Unless it is the employee's assigned job responsibility, providing information about or lists of Town employees, customers or voters to acceptable outside parties;
- Individuals who are neither Town Staff nor otherwise authorized individuals, are prohibited from using Town computing facilities;
- Any other use that may compromise the integrity of the Town and its business in any way.

Unauthorized use of the Town's resources is equivalent to the diversion of any other municipal resource. Under no circumstance will the Town computer resources be used for personal or financial gain.

**ACTION:**

Access and utilization of Town information technology assets is a privilege. Individuals suspected of abusing the use of these assets by violation of these guidelines, related regulations, or laws will be subject to discipline (from Administrative Code, Chapter 15, Article 8- Employee Conduct and Disciplinary Procedures and, Article 9 Section 2 "Grounds for Dismissal and Separations" A-T, specifically, J, "unauthorized use of Town property or equipment.)"

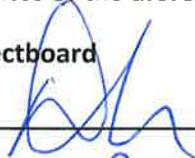
Any employee who is uncertain whether a particular use of information technology assets is permitted should consult with their Department Head. Volunteers should consult with their staff liaison. Final determination as to the appropriateness of any use will be made in consultation with the Town Manager.

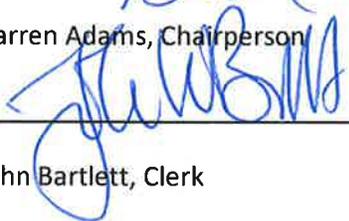
Each employee and volunteer of the Town of Milton using information technology assets as part of his/her position and/or appointment will receive a copy of this Policy. An acknowledgement will be signed and placed in the employee's/ volunteer's personnel file.

**The Milton Selectboard, acting in regular session on December 15, 2014 voted in favor of the following:**

**"Voted in favor of the Town Information Technology Use Standards (2014-04) as outlined above." Further that this referenced Policy shall be part of the permanent record by attachment of the same to the Minutes of the aforementioned meeting."**

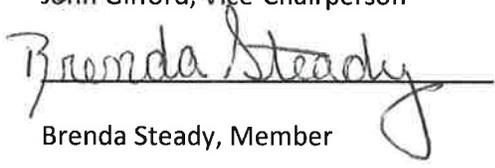
Milton Selectboard

  
\_\_\_\_\_  
Darren Adams, Chairperson

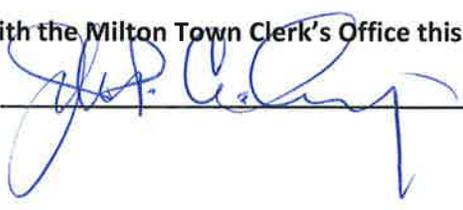
  
\_\_\_\_\_  
John Bartlett, Clerk

\_\_\_\_\_  
Stuart King, Member

  
\_\_\_\_\_  
John Gifford, Vice-Chairperson

  
\_\_\_\_\_  
Brenda Steady, Member

Filed with the Milton Town Clerk's Office this 16<sup>th</sup> day of December, 2014

Attest:   
\_\_\_\_\_