



## Town of Milford

# Technology Acceptable Use Policy

### 1. Purpose

The purpose of the Technology Policy is to create an environment where the Town of Milford's information and resources are secure and in which users of this information understand their responsibilities as users and stewards of these resources and information.

- To safeguard the integrity of computers, networks, and data, either located within the Town of Milford or remote use from elsewhere;
- To ensure appropriate use of electronic communications, technology, and internet use.

### 2. Scope

The technology covered by this policy consists of the Town of Milford voice, data and video networks and all computer equipment, software, printers, copiers and other peripherals provided for use by the Town of Milford. In addition, all Town of Milford-issued or licensed passwords, personal identification numbers, and electronic keys are covered. These resources are the property of, or are licensed by the Town of Milford, and are made available for use to Town of Milford staff for the purposes of doing Town of Milford work.

### 3. Usernames and Passwords:

You have been issued ID's and passwords to access systems and data in accordance with your job responsibilities. You have an obligation to protect the security of these ID's and are expected to do the following:

- Refrain from sharing the password assigned to you and ensure that others cannot learn your password. (i.e. do not write it down)
- Create a password that must be at least 8 characters long, and contain characters from three of the following four categories:

**Group**

**Examples**

Uppercase letters	A, B, C ...
Lowercase letters	a, b, c ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals)	` ~ ! @ # \$ % ^ & * ( ) _ + - = { }   [ ] ¥ : " ; ' < > ? , . /

- Understand that you are responsible for **all** activities under your username/account ID.
- If you have reason to believe that your username/account ID or password has been compromised or you have forgotten it, contact the Information Technology Department immediately.
- When vacating computer workstations, sign-off or secure the system from unauthorized use. The System will automatically lock-out the user after 10 minutes of inactivity.

#### **4. Information Security – Storage and Transmission:**

The Town of Milford community members—staff and volunteers – may encounter sensitive information every day - information such as salaries, job data and personal information including home addresses for example. This information is considered confidential by the Town of Milford. All employees have an obligation to the following:

- Access only accounts, files, and data to which you have been given authorized access.
- Secure information that is in your possession. Sensitive information, accessed in the course of doing your job, should be secured. (i.e. covered from view while in process, and locked away when you are absent)
- Maintain the confidentiality of information classified as private, confidential.
- Use the Town of Milford information, or information accessed while working for the Town of Milford, for tasks related to job responsibilities and not for personal purposes.
- No use of email for sending and receiving personal info as defined by 201 CMR 17 Standards:

**(Personal information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal**

identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

- Storage of personal information should be restricted by necessity and kept only in additionally secured network folders accessible only by the Human Resources Dept.

## **5. Administrative Rights:**

The granting of administrative rights to an employee of Town of Milford is a privilege granted to individuals who require this level of access and control in order to do their jobs effectively.

If you have been granted administrative rights, you must adhere to the following requirements:

1. You will comply with all existing technology appropriate use policies of Town of Milford.
2. You will not make changes to any desktop, laptop or other devices not assigned to you personally.
3. You will not install any unauthorized or non-standard software at any time.
4. You will take all reasonable steps to ensure that the desktop, laptop or other end-user device over which you have administrative rights is secured from malware or intrusion.
5. You will have sole responsibility for backing up any data stored to the desktop, laptop or other end-user device over which you have administrative rights.
6. IT Department resources are very limited, complete support and troubleshooting is only provided for the base Town of Milford software setup and for IT approved additional applications. Support for non-approved applications is not available.

Your administrative rights can be terminated at any time by the Director of Information Technology or Town Administrator if the terms of this policy are violated.

## **6. Installation of Software**

Before any software can be used on Town of Milford computers or the network, the software must be virus-tested; you are prohibited from disabling Town of Milford-installed virus protection software. No copy of software may be used on the Town of Milford's computer or

network resources unless approved in advance of installation by the IT department including shareware and software downloaded from the Internet. You are not permitted to make additional copies of any software without express authorization and proper registration of the copy.

It is illegal to make unauthorized copies of software. Copyright laws protect software authors and publishers, just as they protect authors of printed material. Town of Milford does not condone the use of illegally copied software and will not provide assistance and support to users of such software. Use or distribution of unlicensed software is against Town of Milford policy and is illegal.

### **7. General Usage – Business Purposes:**

- Use the Town of Milford e-mail, computers, and networks only for legal, authorized purposes. Unauthorized or illegal uses include but are not limited to:
  1. Accessing files or emails belonging to others;
  2. Destruction of or damage to equipment, software, or work data;
  3. Unauthorized copying of copyrighted materials; or
  4. Conducting private business unrelated to Town of Milford activities.
- Refrain from any activity that might be harmful to systems or to any information/data stored thereon, such as:
  1. Creating or propagating viruses;
  2. Disrupting services or damaging files; or
  3. Making unauthorized or non-approved changes to computer setup or system resources.

### **8. System Resources and Bandwidth:**

Be aware of any conditions attached to or affecting the provision of Town of Milford technology services:

1. Consult with the Information Technology Department for any questions about system workload or performance.
2. Refrain from disrupting our internet service and internal network operations by monopolizing systems, overloading systems or networks with excessive data, or wasting computer time, connect time, disk space, (e.g. through use of Pandora Radio, Skype, TV, Movies, IMDB.com, streaming Netflix.com, News Webcasts, etc.) as well as printer paper, or other resources

For its own protection, the Town of Milford reserves the right to block all internet communications from sites that are involved in extensive spamming and to monitor

employee internet use by means of security software that identifies misuses of internet bandwidth.

### **9. File Sharing**

File-sharing software allows you to search the Internet for music files (MP3) and download them to your computer. Music file-sharing applications such as Kazaa, Grokster, Morpheus, Gnutella, etc., are network-based programs that allow users to download and distribute music files from computer to computer across networks using Peer-2- Peer methods. As online music, movies and other media have become more popular, the issue of piracy and the theft of copyrighted material have increased as well. Companies who own the copyrighted material being pirated are beginning to increase their pursuit of those who are not abiding by the law. By tracking the files being transferred and the users behind the transferring, these companies are increasingly putting pressure on Internet service providers (ISP's) to reveal identities of the computer users who are infringing copyrights.

Individuals may not establish company computers as participants in any peer-to-peer network, unless approved by the Information Technology Director. The unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject you to disciplinary action, up to and including termination of employment, as well as civil and criminal liabilities. Copyright law provides for damages ranging from a minimum of \$750 to a maximum of \$30,000 per work, with an increase to \$150,000 for willful copyright infringement.

### **10. Expectation of Privacy:**

The Town of Milford computing and network resources are the property of the Town of Milford and under its administration and management. Use of these resources is intended primarily for the Town of Milford business purposes. All files, emails, documents, records, data, and metadata contained on Town information technology is a public record subject to public records requests and review. The Town of Milford reserves the right to scan all network traffic and devices, as well as review any information stored or transmitted on this equipment, without notice and notwithstanding any password, upon direction from the Town Administrator or Town Counsel. Such action would be initiated with just cause or upon receipt of a legitimate complaint to the Town Administrator, Town Counsel, or Human Resources Director that would trigger an investigation. This may be by receipt of the Town of a public records request, as part of a duly initiated criminal investigation to comply with a court order, or as otherwise authorized by law. Examples of complaints might include harassment, conflict of interest activities, or suspected misuse of IT equipment or software.