Acceptable Technology Usage

TOWN OF MARSHFIELD

Acceptable Technology Usage Policy

Date issued: 10-01-2009
Revised: 1-17-2012
Authorized by: Board of Selectmen
Next scheduled review: 3-17-2014

Introduction

The Town of Marshfield provides numerous resources to its employees for purposes of data access and communication services. Due to the increased options and liability in accessing this data and the manner in which the data can be utilized, it's imperative that the Town recognize these changes to our technology usage needs and adjust our policies to meet those demands.

The current services provided to personnel by the Information Technology Department (ITD) include, data access via the Internet, VPN systems, mobile communications and data access via wireless Mobile Mesh and Wireless networks. Basic network access through local and wide area networks for computing needs while on the Marshfield Municipal domain is also included. These services are supplied for the performance and fulfillment of job responsibilities.

This connectivity and data access is for the purpose of increasing productivity and not for non-business activities. Any connection to the Internet or to our domain offers an opportunity for non-authorized users to view or access private information if not configured correctly. Therefore, it is important that all connections be secure, controlled, and monitored via the ITD management systems. Also critical to securing communications and data access requires ITD to manage and monitor mobile applications and mobile devices; including Smartphones, Laptops, Palm pilots, Tablets and other devices.

Security of our systems and data is imperative and employees in the Town of Marshfield should have no expectation of privacy while using Town-owned or Town-leased equipment. The Town reserves the right to monitor internet and network usage by employees, including but not limited to internet sites visited, the duration of employees' internet use, and files which have been

viewed, accessed or downloaded. System auditing is in place to ensure we are aware of unauthorized access and any changes to systems or data as may be required by law.

Employees should be aware that information stored on the Town's computer systems is public record. All data created, stored, or retrieved on the Town computer network is the property of the Town. Email transmissions as well as lists of websites accessed by the employee may be automatically stored on the computer's back-up systems and may be accessed by the Town as it deems necessary and appropriate to ensure proper use of resources and conduct routine network maintenance.

The cost associated with ensuring secure access, storage of data received from the internet, emails or data generated from a local workstation or network storage location constitutes a substantial investment factor for Marshfield and should be managed by all users for the intended purposes.

Permitted use

Internet and data connections including e-mail system usage for the Town of Marshfield personnel is primarily for business use. Occasional and reasonable personal use is permitted, provided that this does not interfere with the performance of work duties and responsibilities of users. Occasional use is defined as time allocated for employee breaks and outside departmental work hours. Employee performance is determined by the employee's manager and access privileges are available to those employees who maintain a satisfactory performance status. Employees may use the Town of Marshfield Internet services for personal improvement, outside of scheduled hours of work, provided that such use is consistent with professional conduct and is not for personal financial gain.

Employees may send and receive e-mail attachments that do not exceed 12 MB in size; provided that all attachments are scanned by the Town's chosen antivirus software prior to being opened. Compressed files will not be allowed. Use of personal email systems is not supported and should be avoided whenever possible due to the heightened risk those emails may contain.

Employees may send and receive short text messages with no enclosures for non-business purposes if the technology is adopted and configured for use on Marshfield systems. Personal e-mails from Internet Email accounts should not be read in the office and any personal e-mail received should not be opened on the Town's computer systems.

Prohibited use

Employees shall not use the Town's Internet or e-mail services to view, download, save, receive, or send material related to or including:

- Offensive or disruptive content of any kind. Offensive content includes, but is not limited to, sexual comments or images, racial slurs or other comments that may offend someone on the basis of their , gender, national origin, age, marital status, sexual orientation, religion, or disability.
- Threatening or intimidating material.
- Illegal activities.
- Commercial messages.
- Messages of a religious, political, or racial nature.
- Gambling.
- Sports, entertainment, and job information and/or sites.
- Personal financial gain.
- Forwarding e-mail chain letters, or "broadcast" messages to lists or individuals, subscribing to "list-serves" or "newsgroups" not in line with town business.
- Political campaigning purposes, including attempts to influence ballot questions or to promote or oppose a candidate for public office.
- Spamming e-mail accounts from Town of Marshfield e-mail services or company machines. Spamming is classified as any act which will present your identity or content sent or received in a manner not representative of the originating user or content.
- Material protected under copyright laws.
- Circulating or supplying Municipal data to Town of Marshfield vendors, contractors or clients without authorization from the manager or duly recognized officers

responsible for maintaining such information or data. Storage of Marshfield data on systems outside Marshfield's municipal systems; IE: Cloud storage services.

- Revealing one's password to anyone else, using anyone else's credentials, or impersonating someone else when sending information or utilizing Marshfield connections.
- Open files received from the Internet without performing a virus scan. Disabling of any application or software used to prevent Viruses, Spam, or Intrusion detection is also prohibited
- The download of any file or content not relevant to the users job activities, including Instant Messaging applications IE: AOL's AIM, MSN Messenger, and Yahoo Messenger or for the downloading of music or WAV files.
- The use of portable USB Flash drives unless provided by the Information Technology Department which mandates the use of an encrypted drive.
- The use of privately or personally owned equipment (Laptops or Handheld devices) connected to the Marshfield networks locally or through a Virtual Private Network connection configured for remote access, unless utilized on the Public network connection supplied in certain locations.
- The use of any Wireless Access Point or device used to extend access to or open up the Marshfield Networks.

Responsibilities

Town of Marshfield employees are responsible for:

- Network and Worksite Security: The Locking, Logging Off or shutting down of computers when leaving for lunch or for the day.
- Following suggested Best Practices when asked to leave your computer's on/off prior to going home for purposes of security patching or upgrades.
- To challenge unknown individuals who are attempting to access any systems on the network or who may be in undesignated area's normally off limits. The procedures for performing this duty should be as follows: Any individual observed as suspicious should immediately be

reported to the department head, Information Technology Director and or including police for questioning depending on level of activity observed.

- To maintain confidentiality with regards to all credentials, passwords and access codes used in gaining access to the computer's, Network Data or remote access. The ability to fortify from theft all hardware in your possession. This requires normal and appropriate security planning and diligence when in possession of Marshfield hardware or software, IE: Laptops or data.
- The ability to abstain from inquiries or surveys regarding Marshfield Networks, computer's or data.
- Making all hardware available to the Information Technology Department (ITD) for security updates, upgrades and secure connection configurations.
- Honoring acceptable usage policies for networks accessed through this organization's Internet and e-mail services.
- Abiding by existing federal, state, and local telecommunications and networking laws and regulations when applicable.
- Following copyright laws regarding protected commercial software or intellectual property.
- Minimizing unnecessary network traffic that may interfere with the ability of others to make effective use of Town of Marshfield network resources.
- Not overloading networks with excessive data or wasting Town of Marshfield other technical resources to solve non-business issues.
- Employees shall not allow non-employees access to the computer systems without the permission of the IT Department unless such computers are designated as available to the public. This includes sharing user profiles for temporary or Part time personnel.
- Employees shall not copy programs without the express authorization of the ITD.
- Employees shall not remove computer equipment from the Town building where it is used and installed, make changes to the configuration or add remove hardware currently installed or pending installation without the prior authorization of the ITD.

  Any passwords used to gain access to systems or resources will be surrendered in the event the Information Technology Director requires it. This also includes the MIS Directors duly appointed System Analyst.

Violations

Violations will be reviewed on a case-by-case basis. If it is determined that an employee has violated one or more of the above use regulations, that employee will receive a reprimand from his or her supervisor. If a gross violation has occurred, as determined in the sole discretion of management, management will take immediate action. Such action may result in losing Internet and/or e-mail privileges and other discipline, up to and including termination of employment with the Town of Marshfield. The Town reserves its right to seek restitution from any user for costs incurred by the Town, including legal fees, due to such user's inappropriate use of electronic resources.

Acceptable Technology Usage Acknowledgement

I have received a written copy of the Town's Acceptable Use Policy. I fully understand the terms of this policy and agree to abide by them. I realize that the Town's security software may record for management use the Internet address of any site that I visit and keep a record of network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive will be recorded and stored in an archive file for management use. I know that the violation of this policy could lead to discipline, up to and including dismissal, or even criminal prosecution.

_____

Employee Name Printed:

_____

Employee Signature:

Date: _____