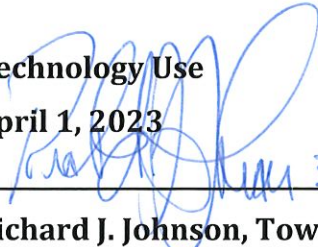


Town of Glastonbury

Administrative Policy No.: 8
Subject: Technology Use
Effective Date: April 1, 2023
Approved By: 
Richard J. Johnson, Town Manager

Purpose:

This policy serves to delineate acceptable uses of the Internet, e-mail, and computer/technology-based systems while using equipment and facilities registered to or provided by the Town. It seeks to ensure that the use of the Internet, e-mail and computer systems by Town employees, appointed/elected officials and others who may be conducting work for the Town while using Town provided systems is consistent with Town of Glastonbury policies, all applicable laws, and the individual user's job responsibilities.

Policy:

The Town of Glastonbury, ("the Town") recognizes the need for technology in the operation of the town and the need to maintain the overall systems in safe working order for all. This policy establishes guidelines for the proper and safe operation of the Technology, Internet, and Email systems in use by the Town.

Privacy: Information is Not Private. Town Computer/Technology systems and the data stored on them is the property of the Town of Glastonbury. All messages created, sent or retrieved over the Internet via the Town's electronic mail systems are the property of the Town of Glastonbury, and should not be considered private information. Users have no right to privacy as to any information or file transmitted through or stored in the Town's Computer/Technology systems, electronic mail, or other technical resources.

Electronic Monitoring: "Electronic monitoring," as defined by Connecticut General Statute (CGS) 31-48d, means the collection of information on the Town's premises concerning users' activities or communications, by any means other than direct observation. Electronic monitoring includes the use of a computer, telephone, wire, radio, camera, electromagnetic, photo-electronic, or photo-optical systems. CGS 31-48d does not permit collection of information which is prohibited under other state or federal law.

Pursuant to Connecticut General Statute 31-48d, the Town of Glastonbury gives notice to all its employees of the potential use of electronic monitoring in the workplace. The Town is authorized to use electronic monitoring when it determines it is appropriate in its discretion.

The following are examples of the types of electronic monitoring which may be used in the workplace:

- monitoring of e-mail, Internet access and other components of the Computer/Technology system, including wireless mobile data terminals
- video surveillance of parking lots, grounds, operational and common areas of Town buildings
- monitoring of any electronic access system for security purposes
- monitoring and recording of telephone and/or radio communications
- monitoring of vehicle location, travel routes, travel history and other similar operating data through Global Positioning Systems (GPS) technology and other vehicle and personal location technologies

Connecticut General Statute 31-48d also provides that the Town may use electronic monitoring without any prior notice when there are reasonable grounds to believe employees are engaged in conduct that (i) violates the law, (ii) violates the legal rights of the Town or other employees, or (iii) creates a hostile work environment.

Questions about electronic monitoring in the workplace should be forwarded to the Director of Human Resources.

Definitions:

Authorized Users: Referred to as Users in this policy include the following;

- Employees, interns, and volunteers
- Elected and appointed officials of the Town of Glastonbury
- Software Vendors that require access to support applications. Vendor accounts will be disabled by default and only enabled while support work is being performed

Computer/Technology: Computer/information technology shall be defined to include electronic-based communication and records, personal computers, software, network servers, e-mail, the Internet, electronic bulletin board systems and other systems and devices that transmit and/or store information on media other than paper

ITM: Information Technology Manager.

Management: Town Manager or designee.

Privileged Access User Account: Certain staff are issued Privileged Access User Accounts. These special accounts have additional rights to install software and configure computer systems. They do not have the same protections for malware and data corruption and therefore cannot be used for downloads or email.

Sensitive Data: Data that contains information of a personal nature such as Social Security number or Drivers License number. Can also include ongoing Criminal Court Records, or HIPPA data.

Standard User Account: Each user is issued a standard login account on the Town Network that is useful for accessing the network, email, and the Internet. The account has built in protections to minimize malware and data corruption activities.

Supervisor: Town Manager or duly designated and authorized department or division director as applicable.

Procedure:

1. Roles and Responsibilities

The Information Technology Department's responsibility within this policy is to provide resources to executive and supervisory staff, which is comprised of the Town Manager and the department/division directors, so that they may administer the policy. Any and all enforcement actions are the responsibility of the Town Manager or duly designated and authorized department or division director as applicable.

Users are expected to observe the same high standards of professional conduct and decorum when using electronic based communications as with other mediums such as telephone, in-person, and written correspondence.

The Town encourages authorized and trained personnel to make use of information technology to improve the efficiency and/or effectiveness of Town services. Town employees are encouraged to be creative in their use of technology and to share this knowledge with other employees.

a. Electronic Messaging

Electronic Messaging includes E-Mail, Texting, Blogging, and other electronic methods of communication in use now or developed in the future.

- i. **Auto Signature Disclaimer:** E-mail messages and the transfer of information via the Internet cannot always be guaranteed as secure. Any employee preparing to transmit information must include the following disclaimer or use the traditional paper mail system:
"This communication, along with any documents, files or attachments, is intended only for the use of the addressee and may contain legally privileged and confidential information. If you are not the intended recipient, you are hereby notified that any dissemination, distribution or copying of any information contained in or attached to this communication is strictly prohibited. If you have received this message in error, please notify the sender immediately and destroy the original communication and its attachments without reading, printing or saving in any manner."
- ii. **Deletion of Files and Email:** No person without specific authorization shall read, alter, or delete any other person's electronic files or e-mail. This applies regardless of whether the Computer/Technology operating system permits these acts. Deletion of all files and emails shall be done in compliance with the current State of Connecticut Record Retention Requirements.
- iii. **Suspected Viruses:** Any user that receives a message from an unknown source or has a questionable attachment from a known source shall not open the e-mail, nor any attachment to that e-mail due to the risk of the attached virus. The e-mail and attachment shall be immediately deleted.
- iv. **Records Retention:** E-mail messages may constitute a public record subject to the recordkeeping requirements of the Connecticut Public Records Program under Connecticut General Statute 7-109 and available to the public

under the Freedom of Information Act. Employees are responsible for printing to PDF on a network drive a copy of any e-mail for which retention of the document is required. (Please see the Town's policy on document retention). Additionally, for the protection of data, all e-mails, documents, and other data are to be saved on the Town's network. If a document is saved elsewhere, it is the duty of the user to preserve the copy and make sure it is available.

- v. **Mailbox Maintenance:** Users are responsible for requesting deletion or destruction of email and electronic documents on an annual basis pursuant to Connecticut Public Records Retention requirements.
- vi. **Program requirements:** Users are to periodically delete unneeded e-mails, documents, and other electronic files that are not subject to public record retention in order to conserve network file storage space.
- vii. **Security Training:** A users of the town's email system will be required to comply with regular training and testing using the town's selected vendor for proper and secure usage of the system.

b. Hardware

Only hardware that has been approved by the Information Technology Department and a user's Supervisor shall be installed for Town use. This includes all Computer/Technology, peripherals and accessories. Only the Information Technology Department or a Departmental System Administrator shall install, uninstall, or relocate hardware. A record of any equipment installed, removed, or relocated by a Departmental System Administrator must be submitted to the Information Technology Department when such action is complete.

Use of Equipment: All Town Computer/Technology and related equipment and products owned by the Town are intended for use only for the Town's benefit. Such equipment is not to be taken off the premises without prior authorization from the users Supervisor. Any movement of the Town's equipment, with the exception of mobile devices, requires prior notification and approval of the Information Technology Department. Additionally, any disconnection or re-connection of Computer/Technology, its component parts, its appurtenances, or its connection to the network is to be performed by or under the supervision of the Information Technology Department.

Use of Audio Output Equipment Connected to Technology: Users shall restrict the use of audio output to head phone and ear plug devices when this technology is required for their job function in areas that would otherwise cause disruption to other personnel.

c. Mobile Devices

Users are responsible for the safety and security of mobile devices (i.e. laptops, etc.) that are assigned to them.

- i. When storing mobile devices in office areas during non-office hours, place them in locked locations such as overhead bins or closets
- ii. Do not leave mobile devices open or unattended in public areas
- iii. When transporting mobile devices in vehicles, use weather resistant padded cases and store in a concealed location such as the trunk
- iv. Do not leave mobile devices in vehicles during extremely cold or extremely hot weather
- v. Do not check mobile devices as baggage when traveling via air or land
- vi. Maintain complex passwords on all user accounts on mobile devices and rotate password compliant with town rotation policy where applicable

d. Privileged Access

Privileged Access to Computer/Technology: Information Technology employees and other designated staff members who provide technology assistance will be provided with a Privileged Access User Account. Privileged Access User Accounts are to be used only when necessary for an appropriate job task. Normal Computer/Technology operations are to be performed with their assigned Standard User Account. All Privileged Access User Accounts must be approved by the ITM prior to creation. In addition, Privileged Account access will require multifactor authentication access each time a privileged access login occurs.

While using the Privileged Access User Account access to the Internet and email is not allowed. Browsing the Internet and downloading of any media must be done with the users Standard User Account.

e. Software

Only software that has been approved by the Information Technology Department or approved Departmental Administrator shall be installed on Town systems. Transfer of software applications from one Computer/Technology to another Computer/Technology or storage device on or off site requires the approval of the ITM. All software installed by departmental administrators shall report the installation of the software to the Information Technology Department.

The Town purchases or licenses the use of copies of Computer/Technology software from a variety of outside companies. The Town does not own the copyright to any of this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it for use on more than one computer.

It is the intent of the Town of Glastonbury to adhere to the provisions of the 1976 U.S. Copyright Act, its 1980 Amendments, and the license agreements and/or policy statements contained in software packages used by the Town. All Users shall respect the copyright and proprietary interests of any materials accessed through the Town of Glastonbury technology resources. Users may not duplicate copyrighted materials, graphics, or software, including Town owned

software, without permission from the copyright holder, unless the use falls within the legal parameters of the Fair Use Doctrine, whether for personal use or for the use of others. The improper duplication or use of copyrighted materials is a violation of this policy and is subject to the disciplinary action, as well as possible civil liability and criminal prosecution.

All software media, Installation information, and licensing requirements must be provided to Information Technology and entered into the TEAMS, Technology Equipment Management System), system for Reporting and Tracking.

f. Remote Computing

Users that are granted remote access to the Town network are responsible for the integrity of the equipment that is used to gain access. The user must verify that such equipment will have current anti-virus software in place and be virus free prior to connection to the town network. The user must ensure that the computer is current on windows updates. In addition, all remote access sessions to the town network will require multifactor authentication during login for each connection performed.

g. Websites

The Town hosts and maintains several websites to disseminate information regarding Town services, programs, and resources to community members and staff. Town staff/affiliates must be granted explicit access and permission to add, remove, or otherwise modify content on any Town-owned website. Such content must be limited to Town business/content and conform to the guidelines set forth by the Town Manager, Marketing/Communications Manager, and/or Department/Division Director as applicable. Content posted to Town websites must be responsibly and professionally developed and meet the standards required of all Town communication forums. Additionally, all content posted to the Town of Glastonbury website specifically, (www.glastonburyct.gov), must comply with the Town Website Maintenance policy #2015-2. Staff members who violate these conditions/policies are subject to disciplinary action.

h. Limited Personal Use

Users of the Town's Computer/Technology systems may use these systems for limited personal use for brief occurrences. This is defined as use initiated during non-paid work hours (including e-mail and Internet usage). Examples of non-paid work hours include lunch time and before and after normal working hours. Personal use is governed by this policy. This is a benefit, not a right, and may be limited or discontinued at any time by Management. The Town does not accept liability for any loss or damage suffered by an employee as a result of that employee using the Town's Information Technology systems for personal use. Occasional, limited, appropriate personal use of these systems is permitted when the use does not:

- i. Interfere with the normal operation of the department or work unit

- ii. Interfere with any other user's work performance or have a negative influence on overall employee productivity
- iii. Have a negative impact on the operation of the Town's technology systems
- iv. Cause any additional expense or workload to the Town or department
- v. Compromise the department, or the Town in any way, or create a negative image of employee productivity or generate negative public perception of Town operations or staff
- vi. Violate any other provision of this policy, any other policy guideline, any law/regulation, i.e., HIPAA, or standard of the Town

Computer/Technology equipment used for occasional personal use must be in a location out of the public view.

In limiting personal use, the Town expects employees to exercise the same good judgment they would use in all work situations.

When using the Town's Computer/Technology for personal uses there is no expectation of privacy. Freedom of Information rules may also apply.

i. Maintenance and Protection of Information and Data

All Users are expected to maintain the integrity of the sensitive, confidential and proprietary information that is stored on or is passed through the Town's information systems in accordance with applicable Connecticut General Statutes. Examples of this include:

Personnel information including performance reviews, disciplinary records, and medical records

- Criminal history information, mug shot images, police investigation records, intelligence files, and tactical information
- Names, addresses, or other personal information for which distribution may be restricted by law
- Payment processing information such as Town or customer bank account numbers and credit card information

To protect all sensitive, confidential and proprietary information, (Sensitive Data), all Town personnel shall observe the following practices:

- i. Access to network directories and databases shall be restricted to personnel with a demonstrated "need to know" as determined by the Users Supervisor
- ii. Personal access codes and passwords shall not be shared, even with other Town employees, except in certain instances where it is deemed necessary for a Supervisor to allow access to certain files or proxy to their employees
- iii. All employees are prohibited from allowing unauthorized individuals access to Town Information Technology systems and databases
- iv. Employees shall either lock their computers and portable devices or log off whenever they leave their work area if devices are in an area with public access

- v. Outside of normal job duty performance, no employee shall make copies of information stored on Town information systems without authorization from their Supervisor. This includes printed reports or electronic media such as tapes and disks. Any Sensitive Data stored on removable media or portable technologies, (i.e. Notebooks, PDA's) shall have data stored in an encrypted format.
- vi. No Data pertaining to Credit Card or Bank Account information for customers, businesses, and residents will be stored in electronic format of any kind
- vii. Employees using mobile Windows based devices will be responsible for connecting devices to town network on a twice monthly basis to install required security updates.
- viii. Periodic review of data files under an employee's purview will be performed to remove any data that as no longer needed with a special emphasis on Sensitive Data, with a one-year minimum review.
- ix. Documents that contain Sensitive Data should not be located on a removable device such as a flash drive or a laptop computer if possible. If required, all storage media for files must utilize drive encryption for added protection along with authorization from Management and the ITM.

Users are prohibited from encrypting or password-protecting computer files without authorization from their Supervisor. (At least two employees shall have access to any protected or encrypted file).

Protection and Viability of Data: Data files created and used by Town staff become critical for normal operations and as such must be adequately preserved via appropriate backup and restore procedures. All applicable data is to be stored on network storage devices such as file servers where daily and weekly backup methods are in place. Storage of data on local workstations, floppy disks, and flash drives are to be avoided except for secondary copies and data transfer to other locations.

Special Computing Environments

Special areas such as Police Computer Forensic labs are not subject to these same rules and policies while performing those functions, but instead are governed by local department rules. These special computing environments are not to be interfaced or otherwise linked to any Town network or equipment without approval and oversight of the Information Technology Department.

2. Restrictions

The Town prohibits the use of Town Computer/Technology resources in the following circumstances:

- a. By unauthorized persons
- b. Personal profit-making activities for personal gain

- c. Political activity
- d. Accessing or transmitting obscene language, sexually explicit materials or materials that disparage any person, group or classification of individuals except as required for official business and as duly authorized
- e. Any harassing, threatening, defamatory, false, inaccurate, abusive, discriminatory, or offensive use that violate the Town's workplace conduct standards or Town, State or Federal Human Rights legislation
- f. Disseminating "chain" type messages and unsolicited bulk messages (Spamming)
- g. Unauthorized installation of any software on Town equipment
- h. Defeating or attempting to defeat, through action or inaction, the security system that is set up to protect the Town's or other computer systems, unless specifically authorized to do so as part of a user's official duties
- i. Installing or using file sharing programs, especially those programs which circumvent the Town's security systems
- j. Installing or using "backdoor" communications to the Internet such as modems, wireless network cards, or access points connected to Town equipment or the Town network
- k. Any use that disrupts the work or actions of other Users
- l. Modifying or deleting another Users' files without explicit authorization
- m. Any use that is wasteful of computing resources or that unfairly monopolizes resources to the exclusion of others
- n. Wasting limited resources, including paper
- o. Misrepresenting oneself as another user
- p. Intentionally infringing upon the intellectual property rights of others and computer programs or electronic information, including plagiarism and/or unauthorized use or reproduction
- q. Any use or action that violates Town Policies, Local, State, or Federal Laws
- r. Users are prohibited from encrypting or password-protecting computer files without authorization from their Supervisor. (At least two employees shall have access to any protected or encrypted file).

Discipline

The Town is aware that violations of this policy may occur under circumstances where the user is involuntarily routed to sites containing inappropriate information or material. Upon arriving at such sites, it is the responsibility of the user to immediately exit such site. The Town is also aware that commercial vendors may secure E-Mail addresses of Users and use these addresses to propagate or otherwise deliver viruses, worms, commercial advertisements, solicitations, etc., under circumstances where the user has no control, intention, or desire to access or transmit the offending information or material. Accordingly, disciplinary action under this policy shall only result from willful intentional violations of this policy. Notwithstanding, the Town reserves the right to discipline any user for violations of this policy where it is apparent that the user knew, or should have known, that violations of this policy were likely to occur as a result of the actions, or inactions of the user in question. Further, to the degree possible, Users should take appropriate steps to discourage and/or prevent further

unwelcomed deliveries or transmissions, including, if necessary, reporting the situation to the Information Technology Department so that appropriate steps can be taken to prevent further inadvertent and unintentional violations of this policy.

Employee's Duty for Notification

Users learning of any misuse of hardware, software or related systems within Town departments shall notify their Supervisor or the Human Resources Department.

This policy is intended to identify and establish policies and procedures for use of the Town's technology systems. It is recognized that not every use or situation can be anticipated in such a policy. All Users are expected to use their best professional judgment when using the Town's technology systems. When in doubt or if questions arise as to reasonable and appropriate use, the User should consult as follows:

- Employee: Consult Supervisor or the Human Resources Department
- Elected or Appointed Official: Consult Town Manager
- Vendor or Consultant: Consult the ITM

Abuse, misuse, or other actions contrary to the best interest of the Town or in violation of this policy will result in disciplinary action up to and including termination of employment for employees, revocation of contracts for non-staff Users working via contract, or revocation of User privileges for elected or appointed officials.

Related Regulations, Policies & Procedures, and Forms¹

Network Security Policy	PCI Data Security Standards
Social Media Business Use	Social Media Personal Use
Admin Policy 2015-2 Town Website Maint.	

Last Reviewed/Updated: March, 2023

Next Review Scheduled: March, 2025

Replaces Administrative Policy #2012-01, Technology Use, Internet, and Email, February 2012

¹ This table references documents that are material to understanding this policy, requirements, or procedures. *Italicized* entries are either presently undeveloped or unknown.