**Town of Branford**

**Information Technology Department**

**Information Technology Policies**

****

Debi Mirto

Director of Information Technology

October 2022

The Town of Branford provides its employees with a variety of information technology resources. These resources include computers, software, printers, mobile devices, telephones, voicemail, and on-line capabilities. The Town provides these Information Resources in order to permit the delivery of better and more efficient services to the Town and its citizens. These resources should be used for appropriate business purposes only.

This policy applies to all users of the Town’s Information Resources. It is the responsibility of all users to read, understand and follow the terms of this policy. Users are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of the Town’s Information Resources.

The content of this document is subject to regular review based on input from the Town of Branford’s Information Technology department as technology changes and advances.

**Use of any of the Town’s Information Resources by any user shall constitute acceptance of the terms of this policy and of any future amendment.**

**Prohibited Activities**

All information resources and data on The Town of Branford’s computer systems are the property of the Town of Branford. This information should be used for appropriate business resources only. The following list of activities are a minimum subset of prohibited activities.

The Town of Branford prohibits employees from:

Uploading, downloading, printing, transmitting, and viewing any information (image, sound,

program, or document) that could be deemed offensive, derogatory, harassing, on the basis of:

* Race
* Gender
* Nationality
* Sexual Orientation
* Religion
* Political Belief
* Disability
* Age

Uploading, downloading, printing, transmitting, and viewing any information (document, image,

sound, or program) containing the following without authorization:

* Copyrighted, trademarked, or patented materials
* Other marked confidential, private, or proprietary information or materials, including all

non-public material.

Using Town of Branford’s computers to:

* Forge (or attempt to forge) e-mail messages
* Obtain unauthorized access or tampering of other users’ email
* Send harassing, obscene or other threatening e-mail to others
* Send unsolicited junk mail, “for-profit” messages, or chain letter messages
* Gain unauthorized access to any computer system, including remote computers
* Damage, alter, or disrupt any computer system, including remote computers or

other systems in any way

* Participate in illegal activities
* Decrypt system or user passwords from any computer system, including remote

computers or other systems in any way

* Copy system files from any computer system, including remote computers
* Copy copyrighted materials, such as third-party software, without the expressed

written permission of the owner or the proper license

* Intentionally attempt to “crash” network systems or programs
* Attempt to secure a higher level of access on the Network
* Knowingly introduce computer programs into the Town’s network
* Knowingly introduce computer viruses into the Town’s network or into external Networks
* Solicit business, sell products, or otherwise engage in commercial activities other

than those required by their job responsibilities

* Using another user’s ID or password without authorization
* Allowing system access to non-employees or any outside personnel without supervisor’s and Information Technology’s permission
* Jeopardizing or breaching the security of the Town’s computer systems in any way
* Excessive internet usage for non-Town related matters
* Tampering with any Town owned computer systems in any way

**Any other activity that is not specifically related to the normal day to day operations of the employee’s position, title, responsibilities, or activities is prohibited.**

**Information Ownership**

All information, data and documentation gathered by, generated by, or provided by Town of Branford employees, in the course of their employment are the property of the Town of Branford. The Town of Branford has legal ownership of, or rights to, the contents of all files, information and messages stored or transmitted on its computer and network systems and reserves the right to examine all data stored in or transmitted by its computer and communications systems, without prior notice, whenever there is a business need which includes, but is not limited to, any investigation of unauthorized or inappropriate use of the systems or other investigation conducted with a business purpose. The use of encryption, the labeling of an email or document as private, the deletion of an email or document, or any other such process or action, shall not diminish the Town’s rights to examine and review such information in any manner, as stated above. Unauthorized use of encryption to prevent management from gaining access to a computer related resource is prohibited.

**Incident Reporting – Data Breach**

Any suspected unauthorized access, theft, data breach or exposure containing data or sensitive data must be immediately reported to the IT Department. This also includes the loss or theft of any devices containing data such as computers, hard drives, thumb drives, smart phones, and data disks.

The IT Department will work with the First Selectman, Human Resource and Legal Departments to determine the appropriate actions to take to protect the data, investigate, and the appropriate communication of the breach.

**User Access**

All requests for new access privileges on the Town of Branford’s systems or networks must be submitted through the Human Resources Department and authorized by the employee’s Department Head. The privileges granted will remain in effect until the user's job changes or when they leave the Town of Branford. If either of these two events occurs, the Human Resources department must notify the IT department immediately.

De

**Change of Status**

Any change in the employment status of an employee must be immediately reported by the Human Resources department to the IT department. When an employee leaves the organization, all system privileges and access to Town information will cease immediately unless specifically authorized by the First Selectman or Director of Human Resources or his/her designee. All electronic/digital files created by an employee for the Town of Branford is Town property and will remain with the Town when the employee departs. Departing employees are prohibited from erasing or discarding any work completed as part of their employment with the Town. All Town owned assets (laptops, mobile devices, hardware, etc.), used outside of the Town of Branford’s offices must be returned to either the employee’s Supervisor, Human Resources or the IT department prior or on their last day of employment.

**User ID’s**

Each employee will be assigned a unique user ID. All user IDs must be constructed according to the IT departments’ User ID construction standard and must clearly indicate the responsible individual's name. This user ID identifies the employee’s security access to specific departmental files and resources. User ID’s will be disabled when employment ends. Re-use of user IDs is not permitted with the exception of re-hiring as informed by the Human Resources Department.

**Password Policy**

All network system user IDs must have a password to ensure that only the authorized user is able to utilize the user ID. Every user ID and related password is intended for the exclusive use of a specific individual; passwords are confidential and must not be shared. Users will be required to change passwords on a periodic basis and will not be able to use recent previously used passwords. Employees must change their password immediately if they suspect that it has been discovered or used by another person. Users must notify the IT Department if they suspect that a password or ID has been compromised.

**Users are responsible for all activity that takes place with their user ID and password or other authentication mechanism.**

**Assigned Equipment**

All hardware, software, mobile and communication devices required by a user to perform their job must be approved by the employee’s Department Head and the IT Department. Employees will ensure that all computer and communication assets that are assigned to or regularly used by them are maintained and used in a manner consistent with their job function and that the possibility of damage and/or loss is minimized. Damage to or loss of Town owned equipment caused by negligence and/or violation of this policy may result in the responsible party being charged for the repair or replacement costs. Employees must promptly report to their supervisor any damage to or loss of Town owned equipment, software, or information that has been entrusted to their care. Computer equipment and software provided by the Town must not be altered or added to in any way without knowledge or authorization of the IT department. Requests for changes to equipment or software must be submitted to the IT department.

**Remote Access**

Remote access to the Town’s internal network will not be granted to any employee by default. Remote users must be authorized through the appropriate request process and subject to a controlled environment. Town employees with remote access capability are required to use their unique ID’s and adhere to security policies and procedures governing the environment. Employees working on Town business via remote access must use Town provided devices unless other equipment has been approved by the IT department as being compatible and secure.

**Internet Use**

Internet access, which is available on Town computer resources, is intended for work related tasks. The Town of Branford uses a web filtering service and any website which has been deemed inappropriate (i.e., pornographic, racial, illegal, or not ethically responsible, etc.), will be blocked. Certain departments who need specific unfiltered web access for their tasks will be granted such after it is signed off by The Director of Technology and The First Selectman or his/her designee. The IT department will view web traffic by employees if a virus or suspicious activity is detected or as directed by an employee’s Supervisor, Human Resources or First Selectman’s office.

**Email and Messaging Use**

Employees must not use any email addresses other than their official Town of Branford assigned

email address for all Town related business matters. Employees must not create, send,

or forward any email, instant messages or text messages that may be considered defamatory, harassing, or explicitly sexual, or would likely offend someone based on race, gender, nationality, sexual orientation, religion, political beliefs, or disability, or that may contribute to a hostile work environment.

The usage of Town computer systems for the transmission of any type of unsolicited bulk email advertisements or commercial messages is strictly prohibited.

Town assigned email addresses should never be used to subscribe to any email lists that

are not directly relevant to an employee’s assigned job functions. It is prohibited to use Town assigned email addresses for personal communications (i.e.: banking, credit cards, shopping.)

Employees should have no reasonable expectation of privacy when using email. All Town email and forms of messaging is subjected to Freedom of Information Act (FOIA) audits. The Town of Branford reserves the right to monitor, access, and disclose all Town employee messages. All Town email and forms of messaging will be treated as business records that may be retained and used as evidence in litigation, audits, and investigations.

**Public Records and Freedom of Information (FOIA)**

Any recorded data or information relating to the conduct of the public's business,

prepared, owned, used, or received by a public agency, whether such data or information

be handwritten, typed, tape-recorded, printed, Photostatted, photographed or recorded by

any method, is subject to disclosure under FOIA unless otherwise protected or

exempt from C.G.S. or federal law. Town assets such as computers, phones, cell phones,

etc. are subject to disclosure under these FOIA regulations.

**E-Mail Etiquette**

Employees are expected to use their access to electronic mail in a responsible, informed, professional

manner. Unsolicited e-mail should never be opened but marked as junk or spam and or deleted.

Never open an attachment if you do not know the source. Confidential information should

never be sent via e-mail.

**Multi-Factor Authentication (MFA)**

MFA is a method of authentication that requires more than one verification method. With new technological advances, it is easy for individuals to inadvertently fall victim to highly sophisticated phishing attacks. The IT Department has taken several steps to protect and monitor the Town network. As part of its efforts, you may be required to use a second device such as a cell phone to establish your identity when accessing certain secure applications. The MFA system will send a message to the device, which the individual must use to authenticate. Upon successful completion of this 2-step authentication process, the individual will be able to access the system. This process will be reviewed and updated as technology changes and may be modified at any time by the IT department.

**Computer Viruses**

Anti-virus programs will protect all network devices susceptible to computer virus infestation. Any user who suspects infection by a virus must immediately shutdown the involved computer, disconnect it from the network and Internet and immediately contact the IT Department, Employees should not attempt to remove the virus on their own. Users must exercise extreme caution in downloading and executing any files attached to email and should contact the IT department if any questionable file or application needs to be downloaded or installed.

**Critical Data Location**

Town business data, especially data that is considered confidential or critical should never be stored on an employee’s local workstation hard disk drives This type of information must reside on security protected server shares, which are backed up nightly. Employees will be assigned individual and departmental shared server folder locations when authorized by their supervisor or the Human Resources department for network access.

**Security Awareness Program**

All Town employees accessing the computer network, or any form of electronic information systems, will be required to participate in a security awareness program to have the necessary skills to carry out their assigned duties in a safe and secure manner. Security Awareness training will be ongoing and new employees are required to participate in an initial training within 30 days of their effective date of hire.

**Public and Employee Wi-Fi access**

The Town of Branford has installed Wi-Fi Access Points in Town buildings and other areas where applicable. Two networks have segmented the Wi-Fi in most locations: one for use by Town employees and one for usage of the public. When utilizing Wi-Fi on Town resources and for work related purposes, employees should connect to the Town’s secure Wi-Fi network only.

**Disclaimer – Usage of PUBLIC WI-FI**

This service is an open network provided for your convenience, and ITS USE IS AT YOUR OWN RISK. It is available to the public and is NOT INHERENTLY SECURE. The Town cannot and does not guarantee the security, privacy or confidentiality of your data and communication while using the Service. The Town does not warrant that the Service will be uninterrupted, error-free, or free of viruses or other harmful components.

If you decide to access any Internet content utilizing Public Wi-Fi, you do so entirely at your own risk, and you are responsible for ensuring that any accessed material does not infringe on the laws governing copyright, trademark, pornography, defamation, or slander.

**Conditions – Usage of PUBLIC WI-FI**

By using this Service, you also agree to the following conditions:

Release and Indemnity. Under no circumstances shall the Town, its officers, employees or agents, be liable for any direct, indirect, incidental, special, punitive or consequential damages or lost profits, whether foreseeable or not, that result in any way from user’s use of or inability to use this Service or to access the Internet or any part thereof, or user's reliance on or use of information, services or merchandise provided on or through this Service, or that result from mistakes, omissions, interruptions, deletion of files, errors, defects, delays in operation or transmission or any failure of performance. You agree to release the Town, its officers, employees and agents, and to indemnify and hold harmless the same, from any claim, liability, loss, damage, cost or expense (including, without limitation, reasonable attorney’s fees) incurred by you or any third party arising out of or related to your use of or inability to use this Service, any materials downloaded or uploaded through this Service, any actions taken by you in connection with your use of this Service, any violation of any third party’s rights or any violation of law or regulation or any breach of this agreement. This Service and any products or services provided on or in connection with this Service are provided without warranties of any kind. All warranties, conditions, representations, indemnities and guarantees with respect to the content or Service and the operation, speed, functionality, qualifications or capabilities of the services, goods or personnel resources provided hereunder, whether express or implied, arising by law, custom, prior oral or written statements or otherwise (including, but not limited to any warranty of satisfactory quality, merchantability, fitness for particular purpose, title and non-infringement) are hereby overridden, excluded and disclaimed.

**Policy Violations**

Non-compliance with these and other information security requirements or any attempt to violate the provisions of this policy may result in disciplinary action up to and including termination, regardless of the success or failure of the attempt. Depending on the severity of the offense, the action may result in the following:

In the case of Town employees:

* Suspension of usage privileges
* Verbal and/or written reprimands
* Disciplinary action
* Discharge of employment
* Legal action as warranted

In the case of Third-Party Personnel, Contractors, or Temporary personnel.

* Suspension of usage privileges
* Termination of access and/or contract or access to the Town’s premises.
* Legal action as warranted.

Specific actions will be taken at the discretion of the Town of Branford’s Management.