Town of Orangetown
ADMINISTRATIVE POLICIES AND PROCEDURES

DEPARTMENT: Information Technology | Policy Number: 2019-T01
SUBJECT: Town Network, Email and Internet Use | Date Issued: 6/4/2019

I. POLICY STATEMENT

The Town networks, which includes internet and intranet access, DMZ (free-wifi) accessed with individual owner devices (BYOD) and the electronic mail (e-mail) systems, is the property of the Town of Orangetown. Accordingly, the Town reserves the right to review any materials transmitted across or stored in computers attached to the network. Any work related posting to the internet or intranet or Email system is a professional communication in your capacity as a Town employee. The tone must be professional and the content must be accurate. Every internet posting and e- mail message must be considered the same as a signed letter written on Town letterhead.

II. APPLICABILITY

This procedure applies to all full-time and part-time Town employees, contractors, and volunteers connecting to the Town network.

III. INTERNET & EMAIL FILTERING

The IT Department will install and maintain filtering software for all Town computers. Internet filtering of Town computers is in accordance with the prohibited uses described in Section V. The filtering of Town computers does not relieve persons from the requirements specified in this procedure, nor does it provide a defense to violations of this procedure.

The IT Department also maintains SPAM filters which automatically filters for and removes suspect or dangerous email from delivery and may place them into a SPAM folder. Incoming email that could be interpreted as SPAM may include, but is not limited to, unacceptable file extensions (such as .zip files), excessively large size file attachments, objectionable content based upon subject title, and recognized malware or virus signatures. End users are provided the capability to manage via email.

IV. SECURITY OF THE TOWN OF ORANGETOWN COMPUTER

Email Usage

In order to prevent system overload and introduction of vulnerabilities into the environment, Town employees must limit the use of the following features to work-related purposes, including but not limited to: transmission of e-mail messages to a large number of

Town employees, or clicking on internal or external URL links in emails. URL links in emails pose a risk of linking to a malware site that could introduce security threats to the Town's network. Town-wide notifications or messages shall have the approval of a department director/office administrator or a specified designee. Notification methods must follow approved delivery methods based upon the need.

Accountability

Users are responsible for the use of their account and any other Town related network/internet accounts and should take all reasonable precautions to prevent unauthorized persons from being able to use their account. No one shall share their passwords. Passwords should not be written or stored in plain text on their computer. All passwords shall follow applicable Town password management standards. It is the responsibility of every employee to report suspected security breaches immediately to IT by contacting IT to report a suspected breach.

Posting or Transfer of Sensitive or Confidential Information

Sensitive or confidential information that needs to be protected for governmental business, legal or regulatory reasons must not be posted on the internet or transmitted insecurely. Town employees are prohibited from sending any message or posting any information as a Town employee or acting on behalf of the Town, implied or intentional on the internet, personal or otherwise, that is contrary to the positions of their department or policies of the Town, unless such messages are for the purpose of reporting improper or illegal actions of Town employees.

V. OWNERSHIP & MANAGEMENT OF TOWN INFORMATION

These include, but are not limited to, network equipment, e-mail, documents, spreadsheets, calendar entries, appointments, tasks and notes which reside in part or in whole on any Town computer system or equipment. Accordingly, information stored on such systems or devices is also Town property and subject to review at any time. There is no privacy when using Town computer resources, and employees have no expectation of privacy in the use of such resources. Electronic mail records are accessible by IT staff to support system performance measurement, tuning, and troubleshooting.

Additionally, HR and the Police Department may have reason to review the electronic files of employees, which may be shared with others as necessary for legal and/or policy enforcement reasons. All Town department directors shall work through the Police Department or HR to evaluate the need to review electronic records of an employee pursuant to an investigation. The Police Department or HR may then request permission from the Town Board for the retrieval of the records, and forward that permission to the DAS (Director of Automated Systems) or designee for processing. In the event an employee

is unexpectedly unavailable for other than disciplinary reasons and access to the employees records is needed to support the ongoing operation of the business, the department director may request access to the electronic records from the DAS or designee.

Departments should coordinate with HR and the Police Department pursuant to applicable Town administrative procedures. Because internet e-mail passes through many computer systems en route to the recipient, it is accessible by others and is not a secure means of communication. When communicating with others, either through the Town computer system on the internet, through email, or other electronic communications means, users represent the Town or Orangetown. The information transmitted or received can be traced and/or reported back to the Town. As with any other data (whether for citizens or employees), computerized information maintained by the Town is subject to federal, state and local laws. Any Town business e-mail or other communications, regardless of origin, may be subject to disclosure under the FOIL, the Privacy Protection Act, and judicial subpoena. Since privacy cannot be assured within non-secure email systems, confidential information shall not be transmitted by e-mail.

VI. USE OF THE INTERNET AND E-MAIL SYSTEM

A. **Acceptable Use** - Employees may use Town computer resources to access the Internet and transmit e-mail messages at any time for work-related purposes. Employees may use the Town computer resources to access the internet and to transmit non-confidential email for appropriate non-work related purposes on personal time in accordance with the conditions governing access to their work areas and at the discretion of department management, as long as there is no effect on public business or job performance and such use is infrequent. This includes the use of personally owned electronic devices while at the workplace, whether connected to the Town network or using a Town publicly accessible Wi-Fi connection. Personal time includes breaks, lunchtime and the time before and after work. In areas where employees must share equipment or resources for network access, employees using the resources to fulfill job responsibilities always have priority over those desiring access for personal use. Use of passive, personally-owned electronic devices (i.e., personal music listening devices such as iPods, etc.) in the employee's work area is left up to the discretion of department management. Use of streaming media (such as Internet Radio) on Town devices is also left up to the discretion of department management, unless it is determined by IT through performance monitoring or problem troubleshooting that its use creates a disruption or problem within the Town network or on an individual work station.

B. **Prohibited Use** - The following activities are prohibited on Town computer resources:

1. Intentionally accessing, viewing, downloading, uploading, posting, or transmitting information that is abusive, offensive, harassing, threatens violence, or that discriminates on the basis of race, color, religion, gender, national origin, age, or disability.

2. Intentionally accessing, viewing, downloading, uploading, posting, or transmitting sexually explicit material. Sexually explicit material includes any description of or any picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting nudity, sexual excitement, or sexual conduct of any kind.

3. Operating a business, soliciting money, product advertising, or conducting transactions for profit or personal gain.

4. Using Town email systems excessively for personal use. Use of Town email is intended primarily for official Town business and personal use, if necessary, should be limited to incidental use and is subject to review and enforcement for abuse and misuse.

5. Gambling.

6. Arranging for the sale or purchase of illegal drugs, alcohol, or firearms.

7. Communication with elected representatives or public or political organizations via Town e- mail to express opinions regarding political issues outside of work-related communications.
8. Solicitation for non-Town sponsored organizations or functions.

9. Sending of Town wide e-mail or e-mail broadcasts without first obtaining approval by the employee's department director/office administrator, and the DAS, or designees. Such messages shall include a statement indicating the person that authorized the message.

10. Reproduction or transmission of any material in violation of any local, state, U.S. or international law or requirement, including material that does not comply with federal copyright laws and copying or reproducing any licensed software, except as expressly permitted by the software license.

11. Using e-mail to transmit sensitive information outside of the Town network to external sources which may include information related to confidential matters, including, but not limited to; protected patient health information, criminal/juvenile records, personnel records, or records relating to legal matters, unless such information is encrypted using IT approved encryption methods and secure file transfer methods. All exchange of sensitive information with external partners requires execution of a Non-Disclosure Agreement (NDA) with the external partner.

12. Intentionally creating a computer virus and/or placing a virus on the Town's network or any other network. Intentionally drafting, forwarding, or transmitting chain letters.

13. Attempts, whether successful or not, to gain access to any other system or user's personal computer data without the express consent of the other system or user.

14. Using the network, internet, intranet, or Email system in any fraudulent manner.

15. Avoiding or circumventing approved email mailbox size and capacity settings as defined by Town Email Guidelines. Each employee's mailbox shall have a quota, which is a control mechanism to limit the amount and/or size of email that can be stored in or sent from the employee's Town-issued email account.

16. Intentionally circumventing security and control features associated with Town filtering policies or other Internet policies by using publicly accessible Internet wireless networks (such as Wi-Fi others) from Town devices for purposes other than approved, official Town government business.

17. Disregarding appropriate application of email or Internet records retention guidelines for the management of Town public records.

18. Inappropriate usage of Social Media or Social Media web sites. Such activities include, but are not limited to:
    a. Posting proprietary, confidential, sensitive, or personally-identifiable information
    b. Speaking on behalf of the Town, or giving the impression of speaking for the Town, when not authorized to do so by the Town Administrator or his designee(s)

c. Speaking on Town-related issues in an unofficial capacity and failing to clarify one's unofficial role of not speaking on behalf of the Town
d. Using tools or techniques to spoof, masquerade, or assume any false identity, except for approved business or law enforcement purposes as approved through Town policy or by legal statute

19. Downloading or installing software without IT approval.

20. Auto-forwarding of Town email which constitutes official Town government correspondence to a personal email account (such as Yahoo, GMAIL, or other internet based email accounts), which reduces the ability to routinely manage the content in accordance with Administrative Procedures.

21. Forwarding of inappropriate email (such as politically sensitive or otherwise offensive jokes, chain letters, or other harassing or spam-like communications) of a personal nature representing a Town correspondence to external Internet email addresses which has the potential to adversely affect the Town's image, reputation, or Internet-based email ethics reputation.

22. Any other use of the network that violates Town of Orangetown policies or Code of Ethics.

C. Email Retention

1. All emails sent to and from Town of Orangetown email addresses are delivered to the recipient's mailbox as well as copied to an email archiver separate from the email system. Clearly stated, each email is saved in two separate, distinct locations. Emails stored in a user's individual mailbox shall have a recommended maximum age of 1 year. Emails stored in the Town email archiving system shall have a maximum age of 7 years.
    a. Voice Mail messaged that are sent to your email and are automatically saved to the archiver will be deleted after 30 days.

2. It is important to note that most emails are NOT records. Most emails are ESI (Electronically Stored Information) without a lasting legal, operational, or historic value. Only emails that serve a legal, operational, or historical value are records, and the rest should be deleted accordingly.

VII. USE OF INTERNET BASED SYSTEMS AND SERVICES

Approval for Use of Internet-Based and/or Internet Hosted Business Solution Systems and Services

Internet-based or hosted systems may be available generally to the public without cost, at a minimal cost, or for more robust versions of the system/service for a significant cost. Regardless whether the system or service is free or requires some costs, authorization to accept Terms of Service (TOS) for Internet-based or Hosted Business Solution Systems or services must first receive approval from the Town's Director of Automated Systems (DAS) and Town Attorney, or their designees. No Town employee is authorized to accept or agree to an Internet-Based TOS without first obtaining this approval.

Internet-based Systems Vendor Management Roles and Responsibilities

Information Technology (IT) has primary responsibility for managing the vendor technology relationship for all Internet-based or hosted Business Solution systems and services for the purpose of assuring appropriate technology practices are applied related to technology architecture, information system security, service level agreements, operational processes, technical support and business continuity.

Information Security Management of Internet-Based and/or Internet Hosted Systems and Services

The Town's DAS has responsibility and approval authority to examine system risks and require appropriate assurance levels of information security controls for all systems, including Internet-Based and/or Internet Hosted Systems and Services, subject to review and approval by the Town Board.

VIII. PASSWORD POLICY

1. Passwords must be treated as confidential information.

2. Passwords must not be included in email messages or other forms of electronic communication.

3. Usernames and passwords are issued to individuals for their exclusive use, and passwords may not be shared.

4. IT and/or management may not have access to your password and may not ask for it. IT may reset your password if they deem that there may have been a security concern.

5. Passwords set by IT shall be set to a temporary password. The users is required to change the password at first log in. IT cannot view user's passwords.

6. Suspected account compromises should be reported to the IT Department immediately.

7. Password format requirements are subject to change.

8. An account shall be locked after 3 invalid login attempts. The account will automatically be unlocked after 2 hours, or by contacting the IT Department.

9. Passwords shall be changed every 120 days.

10. Passwords may not be repeated within one year.

IX. DESKTOP COMPUTER USAGE AND DATA STORAGE POLICY

1. Desktop users must lock their computer or sign out when leaving their desktop computer for a time period of more than 30 minutes.

2. Desktop users must lock their computer or sign out when leaving their desktop computer at the end of each day.

3. Desktop users should not turn off their computer as keeping the computer on allows for Windows, Anti-Virus and other updates to take place in the background during off hours.

4. Desktop users should not store any Town related information on their local computer (C: drive) as this drive is not backed up in any way. Any critical Town information must be saved

on the user's unique drive (for example, "H" drive) or any other departmental drives. Private network drives and Departmental drives are regularly backed up.

5. Personal information (non-work related) may not be saved on your H: drive or departmental drives.

6. Desktop users may not be "local administrators" on their desktop. In the event a software vendor requires a program to run as "local administrator", the IT Department may take any measures deemed necessary to secure the desktop computer.

7. Desktop users experiencing any computer related issues should report the problem to the IT Department as soon as possible.