Town of Union Vale
Summer Staff
Internet, E-mail and Social Media Policy

September 20, 2018

Revision 2.00

Adopted By: The

Town Board

Approved February 18, 2023

E-mail Access and Usage

Each User of the Town's IT System is provided with a Town based e-mail account. Users are provided with storage capacity commensurate with their job function and expected use of the system. When accounts are within 10% of the storage capacity, users will receive a warning message to "clean up". If an e-mail account reaches the storage limit, the sending of new e-mail messages is disabled. Users with a demonstrated need for higher capacity storage limits should contact the Town's IT Manager. Requests showing a work related need will be granted.

The Town based e-mail account is to be used only for purposes directly related to the conduct of official business with the Town and shall not be used for nonpublic purposes including, but not limited to, the pursuit of personal activities, the mass distribution of unsolicited messages, the promotion of commercial ventures, or any political or religious causes.

Users may not create or forward nuisance e-mail, including jokes and chain letters. If Users receive a nuisance e-mail they should send a professionally worded response to the sender, requesting they be removed from the mailing list. If this action is not effective, the User should notify the Town's IT Manager so that additional steps can be taken.

Users of the Town's E-mail system should be keenly aware that they are, at all times, acting on behalf of the Town. All actions and communications should be conducted in the most professional manner possible. Users should be mindful that e-mail statements made to others may become binding commitments upon the Town.

Users should be aware that one of the most common ways of attacking and gaining access to IT systems is by use of "phishing attacks". Phishing is where Users receive an official looking e-mail requesting them to take an action such as clicking on a link or opening an attachment in the message. By clicking on the link or opening the attachment, a malware application is installed on the Users computer that is then used to bypass system security, and in many cases compromise system integrity or do damage to the data contained within.

As previously discussed, the Town's IT Systems contain a great deal of Sensitive and Personal information which could be compromised by a successful phishing attack. For this reason Users should be extremely careful when working with attachments or links within e-mails. Users should not click on any links nor open any attachments in messages from questionable or unknown senders. If the User is unsure if an e-mail is legitimate or not, they should immediately contact the Town's IT Manager before taking any actions.

Phishing attacks are now being used to infect systems with Cryptolocker type viruses. This is where the virus or malware encrypts every file that the infected User has access to. These viruses are especially damaging in network environments where they not only lock all files on the infected user's computer, but also lock every file that the infected user has access to on the organizations network. An infection of a User with high level access can affect thousands or 10's of thousands of files across multiple departments including important applications. An infection like this could expose the Town to embarrassment and / or liabilities.

To limit exposure from phishing attacks, Users may not access their personal e-mail accounts using Town owned computer systems. Users who need to access their personal / home e-mail during work hours may do so using their smart phones. Checking may take place during employee's breaks or lunch periods and should not interfere with the Town's business operations or with the user's ability to perform his or her job function.

Use of Social Media

The purpose of this section of the IT policy is to provide the framework for employee usage of Social Media both inside and outside of the workplace. Social Media in general refers to Internet based applications that allow for the creation and exchange of user generated content. Examples of Social Media include, but are not limited to: Facebook, Twitter, Instagram, Tumblr, MySpace, LinkedIn, Flicker, Imgur, YouTube, web blogs and web based wikis whereby users can add, modify or delete its content via a web browser.

Unless the use of Social Media is pertinent to Town business and authorized by a Department Head, employees are prohibited from using Social Media during working hours. This applies regardless of whether or not such usage occurs on Town-owned devices or a device personally owned by the employee.

The following uses of Social Media are prohibited by all Users at all times, regardless of the location from which the post is made or the device being used.

This list is meant to be illustrative, and not exhaustive.

- Disclosing confidential or proprietary information pertaining to matters of the Town that is not otherwise deemed accessible to the general public under the Freedom of Information Law (Public Officers Law Article 6, §§84-90).

- Matters which will imperil the public safety if disclosed.

- Promoting or endorsing any illegal activities.

- Threatening, promoting, or endorsing violence.

- Directing comments, or sharing images that are discriminatory or insensitive to any individual or group based on race, religion, gender, disability, sexual orientation, national origin, or any other characteristic protected by law.

- Knowingly making false or misleading statements about the Town, or its employees, services, or elected officials.

- Posting, uploading, or sharing images that have been taken while performing duties as an agent of the Town, or while wearing Town uniforms – the only exception to this rule is when it is directly pertinent to Town business and such posting, uploading, or sharing of images is authorized in advance by the appropriate Department Head.

- Representing that an opinion or statement is the policy or view of the Town or of any individual acting in their capacity as a Town employee or official or otherwise on behalf of the Town, when that is not the case.

- Posting anything in the name of the Town or in a manner that could reasonably be attributed to the Town without prior written authorization from the applicable Department Head.

- Using the name of the Town or a Town e-mail address in conjunction with a personal blog or Social Media account.

Social Media (cont.)
An employee's Social Media usage must comply with Town policies pertaining to but not limited to Non-Discrimination and Harassment, Confidentiality, Violence in the Workplace, and Substance Abuse. Any harassment, bullying, discrimination, or retaliation that would not be permissible in the workplace is not permissible between co-workers online, even if it is done after hours, from home and on personal devices.

Notwithstanding the above, nothing in this policy is meant to imply any restriction or diminishment of an employee's right to appropriately engage in protected concerted activity under law.

Anyone with information as to a violation of this policy is to report said information to the appropriate Department Head. Once the Department Head is informed of the violation, a formal process, consistent with this Information Systems Usage Policy, Employee Handbook and/or applicable law, will begin.

Any employee who violates this policy will be subject to disciplinary action up to and including termination of employment.

ACKNOWLEDGMENT OF RECEIPT OF:
TOWN OF UNION VALE'S INTERNET, E-MAIL AND SOCIAL MEDIA POLICY

I, (print name)_____hereby acknowledge that on this date I have received a copy of the Town's Internet, E-mail and Social Media usage policy adopted by the Union Vale Town Board. I hereby acknowledge that I have read and understood the policy and procedures contained therein. I understand that if now or any time in the future I do not understand this policy or procedure, or I have a question about it, or I believe there has been a violation of the policy, that I must contact my immediate Supervisor or Department Head to resolve the situation.

I agree to abide by this policy and specifically understand that violation of this policy may lead to discipline, up to and including termination.

Signature _____

Date _____

Please return this signed acknowledgement to the Finance/HR office.