TOWN OF WEST SENECA

Legal Department

To: Town Board
From: Chris G. Trapp, Attorney for the Town
Re: Policies
Date: May 18, 2022

As a matter of best practices, we are proposing a Acceptable Use policy governing the use of electronic equipment owned by the Town and the use of other equipment along with a Cyber Security Policy which will set the framework for protecting the information of the Town. Both policies are presented for your consideration. No formal action is required at this time pending the completion of your review.

The Town of West Seneca Town Board (the "Board"), recognizes that telecommunications and other technologies are shifting the ways in which information is being accessed, communicated and transferred by members of the society and therefore, the Board wishes to provide Town employees access to various computerized resources through the Town Computer Network (TCN) consisting of software, hardware, computer networks and electronic communication systems, to analyze and evaluate such information.

Goals and General Principles

1. The Board encourages employees to make use of the TCN to explore educational and information topics, conduct research and contact others in the business and municipal world.

2. In order for the Board to be able to continue to make its information resources available, all users must take responsibility for appropriate and lawful use of TCN and other technology. Users must understand that one person's misuse of TCN technology, may jeopardize the ability of all users to access the network and the internet.

3. The Board firmly believes that the valuable information and interaction available using technology far outweighs the possibility that users may procure material that is not consistent with the goals of the Board.

Board Responsibilities

1. The Board, will serve collectively as the coordinator to oversee the use of Town technology systems, or the Board may designate personnel for oversight purposes.

2. The Board reserves the right to revise this Acceptable Use Policy as it deems necessary and will post the current policy on its web site as notice to users of any revisions. Users are responsible for reading the policy regularly.

User Responsibilities

1. Users are responsible for good behavior on the TCN.

2. Various technology, the network and telecommunication equipment is provided for Town employees to conduct research and communicate with others.

3. Access to various technology and network services will be provided to Town employees who agree to act in a considerate and responsible manner.

Listed below are provisions regarding appropriate and responsible use of technology, the computer network and the Internet. If you have any questions about these provisions, you should contact a member of the Board, an immediate supervisor or other personnel designated by the Town. If any user violates this policy, the user's access may be denied or withdrawn and he/she may be subject to additional disciplinary action.

I. Guidelines for Acceptable Use

The main principles defining "acceptable use" are those stated above: to use computing facilities and equipment only for the Town purpose for which they are provided, to show consideration to other users, to respect the privacy of all other users and to obey all relevant guidelines.

New users are required to review the Acceptable Use Policy (AUP). Appropriate user accounts will be created upon the completion and return of the appropriate AUP Employee Signature Page. The AUP Employee Signature Page appears as "Appendix A" below.

Users will be required to review the AUP annually and acknowledge same. User accounts will be maintained upon the completion and return of the appropriate AUP Employee Signature Page. (Appendix A) All town owned devices shall specifically provide notice when an employee signs in that the use of such devices shall only be for Town purposes.

Users are not to unreasonably deprive other users of access.

All users are responsible for immediately reporting any damage or malfunction of any hardware, software, security or other component of network systems to the Board or proper personnel.

Users may use personal computers and other electronic computing devices, including but not limited to cellular telephones, iPads and similar devices, notebooks, all devices set forth in section IX below, and all other pieces of equipment that have internet access, upon the return of a completed Employee User of Personal Electronic Device Agreement. Use of personal computing device follows the same guidelines as school computer when connected to the network. Employee User of Personal Electronic Device Agreement appears as "Appendix B" below.

II. Privacy

TCN technology, including network access and internet access, is provided as a tool for Town employee education. In order to maintain system integrity, the Board reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and internet access and any and all information transmitted or received in connection with such usage. All such information shall be and remain the property of the Town of West Seneca and no user shall have any expectation of privacy regarding such materials.

III. Use of Computer Software and Operating Systems

TCN computer software has been purchased for Town use only and is protect by Federal Copyright Laws. The following guidelines apply to the use of software purchased by the Town of West Seneca.

1. Treat computer software like any other copyrighted material.

2. You may not install software protected by copyright on any Town computer without written permission from the Board.

3. You may not install computer software purchased by the Town of West Seneca on any computer outside of the Town.

4. You may not attempt to modify, reprogram, translate, disassemble, decompile or otherwise reverse engineer any software protected by copyright laws.

5. Software residing on privately owned computers must be personally owned, except in the case of antivirus software and desktop monitoring software used by the Town.

6. Software companies will not be held liable for any indirect, special, incidental, economic or consequential damages arising from the use or inability to use the software.

7. Unauthorized reproduction or distribution of software or information protected by copyright laws or any portion of them may result in severe civil and criminal penalties and may be prosecuted to the maximum extent possible under the law. Furthermore, violations of the above guidelines will result in applicable disciplinary actions and financial charges to remove such software from the computer's hard drive at a charge comparable to current industry standards for service work.

8. Software purchased by Town employees for home use may not be installed on TCN computers unless the license agreement allows for such use.

9. Some exceptions do exist; please contact the Board or appropriate personnel for more information regarding software titles in question.

IV. Unacceptable Use of Technology and/or Network

The smooth operation of any network relies upon the proper conduct of the end-users, who must adhere to strict guidelines. The Town is providing access to its computer network and the Internet for only educational and informational purposes.

If you have any doubt about whether a contemplated activity is educational, you may consult with the personnel designated by the Town to help you decide if a use is appropriate. In general, user responsibilities require efficient, ethical and legal utilization of the network resources. The use of network resources must be in support of the educational and informational goals of the Board. Uses deemed inappropriate include but are not limited to the following:

1. Using obscene language or sending or displaying offensive messages or pictures

2. Harassing, insulting or attacking others

3. Plagiarism and violation of copyright laws

4. Downloading of copyrighted music is forbidden

5. Imaging electronic devices or computer networks

6. Disrupting the intended use of electronic resources

7. Using others'accounts or unauthorized access to network resources

8. Intentionally wasting limited resources

9. Users shall not tie up the network with idle non-educational/informational activities.

10. Users shall not store information, pictures, sounds or movies on Town owned computers that do not support the educational and informational goals of the Board.

11. Using electronic resources for commercial and non-educational purposes

12. Users will not use the Internet for advertising, promotion, commercial purposes or similar objectives.

13. Users will not use the Internet to conduct for-profit business activities or to engage in religious activities.

14. Users are also prohibited from engaging in any non-governmental-related fund raising or public relations activities such as solicitation for religious purposes, lobbying for political purposes or soliciting votes.

15. The Town is not responsible for any other commercial activity users engage in.

16. Vandalizing information –includes, but is not limited to:
    a. The uploading, downloading or creation of computer viruses
    b. Attempting to harm or destroy district equipment or materials
    c. Changing settings on electronic equipment without authorization

17. Revealing personal information about anyone without written permission

18. Violating the law or encouraging others to violate the law through the use of technology

19. Shopping for non-Town related items.

20. Using electronic devices for personal use such as travel plans, personal research, making appointments, reviewing personal business documents.

VIII. Email Usage

1. Users will check their e-mail frequently and delete unwanted messages promptly.

2. "Acceptable"e-mail activities are those that conform to the purpose, goals and mission of the Board and to each user's job duties and responsibilities. Users shall have no right to privacy while using the Town's internet or e-mail system.

3. "Unacceptable"use is defined generally as activities using TCN hardware, software or networks at any time that does not conform to the purpose, goals and mission of the Board and to each user's job duties and responsibilities. The following list, although not inclusive, provides some examples of unacceptable uses:

a. E-mail may not be used for personal purposes during working hours, except that users may engage in minimal email activities for personal purposes, such as family correspondence, if the use does not diminish the employee's productivity, work product or ability to perform services.

b. Using e-mail services for private commercial or business transactions and any activity meant to foster personal gain.

c. Using Town e-mail address to subscribe to websites or other internet services that do not conform to Town educational or informational activities.

d. Conducting non-Town fund raising or public relations activities such as solicitation for religious and political causes or not-for-profit activities.

e. Transmitting threatening, offensive harassing information (messages or images) containing defamatory, abusive, obscene, pornographic, sexually oriented, racially offensive or otherwise biased, discriminatory or illegal material.

f. Attempting to subvert network security, impair functionality of the network or bypass restrictions set by the network administrators. Assisting others in violating these rules by sharing information or passwords.

g. Distributing "junk" mail, such as chain letters, advertisements or unauthorized solicitations.

h. Revealing, publicizing, using or reproducing confidential or proprietary information regarding the Village including, but not limited to, financial information, databases and/or the information contained therein, computer network access codes, employee information and business relationships.

i. Users should contact their supervisors or appropriate personnel about questionable e-mail usage.

IX. Use of Personal Electronic Devices

Employees will be allowed to use personally owned computing devices to access the TCN wireless network. Employees are to use these devices in a responsible, efficient, ethical and legal manner. The Board reserves the right to determine if an employee's use of personal electronic communication devices is inappropriate and may take appropriate disciplinary action. For this policy a Personal Electronic Device is defined as an electronic communication device capable of internet access, word processing and other Town related applications. This may include:

a. Notebook or Netbook Computer

b. iPad or other Tablet Computer

c. small internet devices, including, but not limited to, Game Boy or similar devices

d. iPod, or other digital media player

4. Administration

1. A firewall is a part of the Town's computer network. Its purpose is to protect the confidential nature of the TCN. The firewall logs and documents all traffic between the Town network and the Internet (i.e. user I.D.'s and web pages read). These logs will be used by the Board to research violations of this computer access and usage policy.

2. The maintenance, operation and security of computing resource require responsible members of the Board and/or designated personnel to monitor and access the system.

Disciplinary Action Steps for Failure to Comply

If any user violates this policy at any time, the user's access may be temporarily suspended, or denied or withdrawn immediately and he/she may be subject to additional disciplinary action. The Board maintains complete discretion in assessing violations and violations of the policy are not appealable. All violations will be noted on the employee's user account. If employee's TCN access privileges are revoked, they may be reinstated only by the Board.

Cyber Security Policy

Introduction.

The risk of data theft, scams, and security breaches can have a detrimental impact on the Town's systems, technology infrastructure, and reputation. As a result, the Town of West Seneca has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Purpose.

The purpose of this policy is to (a) protect the Town's data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for municipal and personal use, and (d) list the Town's disciplinary process for policy violations.

Scope.

This policy applies to all of the Town's employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the Town 's electronic systems, information, software, and/or hardware.

Confidential Data.

The Town defines "confidential data" as:

- Unreleased and classified financial information.
- Town resident, supplier, and employee information.
- Information not subject to the Public Officer's Law.
- Operational processes, and/or new technologies.
- Employees' passwords, assignments, and personal information.
- Town contracts and legal records.

Device Security.

Town Use.

To ensure the security of all Town-issued devices and information, Town employees are required to:

- Keep all Town-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 12 characters).
- Secure all relevant devices before leaving their work area.
- Obtain authorization from the Town Clerk and/or Supervisor before removing devices from Town premises.

- Refrain from sharing private passwords with coworkers, personal acquaintances, senior personnel, and/or any other individual.
- Regularly update devices with the latest security software.
- Acknowledge that computer usage is only for town use.

Personal Devices.

The Town recognizes that employees may be required to use personal devices to access Town systems. In these cases, employees must report this information to the Town Clerk for record-keeping purposes. To ensure Town systems are protected, all employees are required to:

- Keep all devices password-protected (minimum of 12 characters).
- Ensure all personal devices used to access Town-related systems are password protected.
- Install full-featured antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

Email Security.

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, the Town requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the Town Clerk regarding any suspicious emails.

Transferring Data.

The Town recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, all employees must:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over Town networks.
- Obtain the necessary authorization from the Supervisor or his/her designee.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Adhere to State, Federal, and local data protection laws and all confidentiality agreements which exist.
- Immediately alert the Town Clerk of any breaches, malicious software, and/or scams.

New Employees.

All new employees shall be provided a copy of the Acceptable Use, Social Media, and Cyber Security policies upon hire and trained on the use of computers in the Town consistent with the policies and procedures currently in place.

Terminated Employees.

Immediately upon any separation from service, whether voluntary or involuntary, all access to Town computer systems for such employee shall be locked and all computers and similar equipment, including both hardware and software, must be immediately returned to the Town. Access through any cellular telephones must also be terminated prior to the employee's departure. Passwords used by such employees should be immediately changed and all remote access blocked.

Disciplinary Action.

Consistent with any collective bargaining agreements and Town policies, a violation of this policy can lead to disciplinary action, up to and including termination. The Town's disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.