TOWN OF OSWEGO

2320 County Route 7 Oswego, New York 13126
Phone (315) 343-2424 Fax (315) 343-4414
Supervisor Richard E. Kaulfuss
Town Board Members: Greg Herrmann, Margaret Mahaney, Victoria Mullen, Richard Tesoriero
Attorney to the Board: Kevin C. Caraccioli

Town of Oswego COMPUTER USE POLICY

Use for official business; prohibited uses.

The Town of Oswego (hereinafter "Town") has adopted the following Town of Oswego Computer, Network Resource and Internet Usage Policy:

A. Town computers, Town network resources, and Internet access lines within the Town Hall, Town Highway Garage, and Community Center and within any other Town buildings are to be used only for official business of the Town. This does not apply to computers set up in the Community Center for use by the public.

B. In no event are those computers, network resources or internet access lines to be used for the purpose of:

(1) Personal activities. However, personal use of the systems is authorized within reasonable limits as long as it does not interfere with or conflict with business use. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. This restriction shall not apply to people using computers set up for the use of the general public in the Community Center but it does apply to Town employees using computers that are set up for Town business work,

(2) Creating, sending, posting, displaying or receiving any pornographic or obscene pictures, text, graphics, images, or materials,

(3) Accessing any Web sites that contain sexually explicit images and/or related materials, advocate illegal activity, and/or advocate intolerance of others,

(4) Creating, sending, posting, or displaying any sexually explicit images,

(5) Advocating or promoting any illegal activity, and/or advocating or promoting intolerance of others,

(6) Creating, sending, posting, displaying or receiving any offensive, abusive, slanderous, libelous, defamatory, vulgar, harassing or intimidating messages, text, graphics, images or materials,

(7) Creating or sending any viruses, worms, hoaxes or chain letters,

(8) Engaging in any unwarranted invasion of the personal privacy of any individual,

(9) Engaging in any unauthorized disclosure of sensitive or confidential information belonging to the Town,

(10) Violating any licensing or copyright restrictions,

(11) Engaging in sexual and other illegal types of harassment,

(12) Connecting unauthorized equipment to the network or computers for any purpose (before any additional device is attached to the Town issued network or computer, prior authorizations should be received from the Town Supervisor or IT Manager),

(13) Running or installing unauthorized software unrelated to job duties on the Town computers,

(14) Using the Town's network to gain unauthorized access to any computer system, and

(15) The Town's systems may not be used to solicit for personal gain or for the advancement of a political or religious belief.

Privacy rules regarding use of the internet by Town employees or officer:

Consistent with applicable federal and state law, the time an employee spends on the Internet while on Town property may be tracked through activity logs or other devices and software by the Town in order to monitor computer usage for business purposes. All abnormal or inappropriate usage will be investigated. For business purposes, the Town reserves the right to search and/or monitor internet usage and the files/transmissions of any employee on Town owned equipment or devices without advance notice and consistent with applicable state and federal laws.

All email passwords must be made available to the Town Clerk and the IT manager at all times and, otherwise, shall be guarded from the use of by others. Passwords for Administrative control that must be shared (such as main server, routers, general admin log-in) and external authentications, e.g. the Town of Oswego website and Facebook page are to be given to the Town Clerk and IT manager and are accessible only by the Clerk and the IT manager. Employees shall not use unauthorized codes or passwords to gain access to others' files. Administration shall schedule overall password changes intermittently. The period between such changes shall not exceed 18 months.

Employees should expect that communications that they send and receive by the Town's email system will be disclosed to management. Employees should know that any email sent from Town computers using Outlook is archived and thus accessible by anyone. Employees should not assume that communications that they send and receive by the Town's email system are private or confidential. Use your assigned Town e-mail for all Town business not your personal e-mail address; however usage of personal email address from Town owned computers has no privacy and may be accessed by the Town. Again, all Town business related e-mails whether on Town e-mail or personal e-mail are F.O.I.L. able (Freedom of Information Law). It is highly suggested that you keep your personal e-mail account separate from your Town account. Employees learning of any misuse of the internet shall notify a department head. Electronic communications on

Town owned equipment include, among other things, messages, images, data or any other information used in email, instant messages, voice mail, fax machines, computers, personal digital assistants, cell phones, text messages, pagers, telephones, cellular and mobile phones including those with cameras, Intranet, Internet, back-up storage, information on a memory or flash key or card, jump or zip drive or any other type of internal or external removable storage drives. Should an officer or employee lose a storage device with Town documents etc. thereon or lose a Town issued computer including “smart phones” or tablet devices or lose personal devices that contain information regarding Town business, this loss should be reported to the Town Clerk as soon as possible.

Town officers and employees must be careful to not open suspicious email or responding to spam emails or opening any suspicious attachments. It is preferable to notify the Town Supervisor or IT manager that you have received something suspicious but you suspect may be harmless and contains Town related material and obtains their approval before opening such. Dangerous emails generally contain wording conveying something that is “too good to be true” and/or contain sentences with bad spelling and grammar and misuse of words. The Nigerian Prince is still out there!

Misuse

Any misuse of a Town computer, network resource, or Internet access line, or noncompliance with the Town's written computer and internet usage policies, may result in one or more of the following consequences:

A. Temporary loss of privileges and/or deactivation of computer/network access/Internet access,

B. Permanent loss of privileges and/or deactivation of computer/network access/Internet access,

C. Disciplinary actions (including proceedings for removal from office) by the appropriate Town Board or Town officials and/or state boards or state officials,

D. Subpoena of data files and/or the application for and execution of a search warrant,

E. Legal prosecution under applicable United States, New York State, and/or Town of Oswego statutes, local laws, ordinances, codes, rules and/or regulations (hereinafter "laws"), and

F. Possible penalties under applicable laws, including fines and/or imprisonment.

User compliance
I understand and will abide by this Computer Use Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

This policy is adopted as of 3/13/2018

_____ _____
Employee signature Date

3.13.2018
This policy will be reviewed annually and revised as necessary.

Computer Use:

Suggestions: Add a line that the policy will be reviewed annually and updated as necessary.

I would add the Cyber Security Checklist will be completed annually.

Wi-Fi password should be changed at a minimum quarterly. Every person using a computer should have a password to sign on. The password should be changed every so often (decided by the board). All passwords should be provided to you in a sealed envelope and kept under lock and key.

No Town Business should be stored on a home computer.

All computers will have virus protection software (Norton).

All computers should be scheduled for a yearly "deep clean" to clean up any virus, etc.

Town employees who chose to not set up an email for town business shouldn't have their email displayed on the website or Town directory – that can be considered promoting the use of one's personal email for town business.

Each computer will have a scheduled back-up with the new back-up system. I think if Dave Sterio brings his computer in and signs in Wi-Fi he can do a manual back-up to the system.

Are employees to sign when policy is updated?

Are you adding the Cyber Protection rider to your NYMIR policy? (This is important when employee's final info, social security #'s, etc. are saved)

Williamson Law software program's all have different password parameters; Code Enforcement can use capital letters, small letters, special characters and numbers, Tax Collection and Town Clerk may not be able to. Same with Highway Superintendent software.

What town position (Supervisor, Clerk, etc) will be responsible for monitoring and maintaining this policy?