Suffield Information Technology Department
(860) 668 3350, 230C Mountain Road, Suffield, CT 06078

Information Technology Acceptable Use Policy

SECTION I: General

The Town of Suffield recognizes the need for computers, electronic communications and Internet access systems and the vital role they play in assisting Town employees in delivering exceptional public services. The Town provides computers, electronic communications and internet access systems as tools and it is expected that these tools will be used in an appropriate manner at all times. The primary purpose of computers, electronic communications and Internet access systems is to assist in the conduct of business with the Town. The Town encourages its employees to use and become proficient in the operation of electronic communications and Internet access, which can improve office efficiencies and the conduct of routine municipal activities. All information and communication on such systems is the property of the Town, and there is no expectation of privacy.

SECTION II: Definitions

Electronic Communications and Internet Access Systems shall include but not be limited to computers, electronic mail systems (e-mail), electronic bulletin boards, internet use, facsimile (fax), telephones, cell phones, radios, walkie-talkies, and communications infrastructure.

Examples of Electronic Communications and Internet Access Systems:

- Electronic messaging
- Internet research
- Meeting notifications and scheduling
- Relaying phone messages
- Calendaring
- Work assignments
- General announcements
- Business related information services, i.e. newsgroups, mailing lists, etc.

Computer – Any computing hardware

Operating System – The software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals

Hacking – The act of using computing hardware to gain unauthorized access to data in a system

Malware – Software intended to damage or disable computers and computer systems

Virus – A piece of code capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data

Worm – A self-replicating program able to propagate itself across a network, typically having a detrimental effect

Trojan – A malicious computer program that misleads users of its true intent with a name derived from the Ancient Greek story of the deceptive wooden horse that led to the fall of Troy

Spyware – Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive

Adware – Software that automatically displays or downloads often-unwanted advertising material when a user is online

Key logger – A computer program that records every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information

Electronic mail – Messages distributed by electronic means from one computer user to one or more recipients over a network; commonly referred to as email or e-mail

Internet Service Provider – A company that provides subscribers with access to the internet

Confidential or Sensitive Information – Information used by Town officials or employees in representing the Town in pending legal matters or negotiations of any type which would put the Town at a disadvantage in the negotiation process should the information be disseminated; this includes personnel information, health information, and financial information regarding any employee of the Town

SECTION III: Operational Standards

The use of electronic communications and internet access is intended for official Town business. Any electronic communications and internet usage on Town equipment and software is, by law, public information and may be monitored by the Town as stated in the Section XI: Monitoring of Computer/Communications Activity. All users are reminded that electronic communications and internet access is subject to all applicable Federal, State, and local laws, regulations, ordinances, or policies. Employees are responsible for observing copyright and licensing agreements that may apply when downloading files, documents, software and images.

SECTION IV: Moving Equipment

The Information Technology Department may grant specific exceptions to this policy based on organizational needs and resources. Most importantly, improper connections to certain hardware components can affect the entire network. All equipment shall be moved, assembled, or otherwise configured by the Information Technology Department staff. Any peripheral equipment shall be installed, attached, or otherwise configured by the Information Technology Department staff. This is essential in maintaining network performance and troubleshooting and resolving network problems. Updated inventories are important in planning future technology enhancements including hardware upgrades, changing software applications and implementing new technologies.

SECTION V: Security Practices

End users have a responsibility for security. This includes maintaining the integrity of security profiles by not releasing passwords to other employees or persons, visually displaying passwords, and not

leaving workstations unattended while logged in and unlocked. Employees may need to change their security profile periodically to ensure security integrity. The Town reserves the right to bypass individual passwords at any time and to monitor the use of the system by employees. Users must not interfere with the work of others or with the performance or otherwise intended function of the computer hardware or software. These actions include but are not limited to: attempting to elicit, access and/or use passwords, creation of additional unauthorized users or passwords, entering restricted areas of the network, or inappropriately accessing or altering Town records.

The Town of Suffield reserves the right to limit or deny access to certain Electronic Communications services as a security precaution during electronic virus/worm outbreaks, any credible threat of attack against the Town's network, or in an ongoing investigation. As a result of such measures, the Town's Information Technology staff does not guarantee availability and quality of service of third party communication services (web e-mail, etc.).

All employees, officials, vendors/contractors, and volunteers who are granted access to the Town of Suffield computer/communication systems will be required to sign an Acceptable User Agreement indicating the employee, official, vendor/contractor, or other volunteer has received a copy of the Town of Suffield's Information Technology Acceptable Use Policy and that they agree to be bound by said policy.

Employees shall be required to change their password every 180 (one hundred eighty) days in order to preserve the security integrity of our communications systems. Newly created passwords will be required to meet the following security requirements:

- The password must meet the complexity requirement of having three out of four of the following:
    - An uppercase letter
    - A lowercase letter
    - A number
    - A special character
- The password must be at least 9 (nine) characters in length
- The password must not match the last 10 passwords used with the account

In the event the employee is unable to enter their password correctly 6 (six) times, the employee will be locked out and will be unable to attempt to log in again for 10 (ten) minutes or until the Information Technology Department is contacted to unlock the account.

SECTION VI: Procurement Process

All procurement requests shall be submitted to the technology support staff for review and approval. This is required to ensure appropriate standardization of products and technology to facilitate support, operational performance and training. Hardware and software components may have issues of compatibility with various hardware and/or software configurations and must be reviewed in order to ensure proper integration into our electronic systems.

Proper procurement procedure is as follows:

1. The employee shall provide the Information Technology Department with a Support Ticket (see Section XIII) detailing the item(s) they wish to purchase.

2. An employee of the Information Technology Department will research any equipment prior to purchasing to ensure security guideline compliance and compatibility with existing infrastructure.

3. The Information Technology Department will provide approval for the purchase or alternatively suggest a more fitting solution if available.

The Information Technology Department reserves the right to reject the responsibility of providing maintenance, support, or installation of any hardware, software, or other electronic device in the event an employee or department chooses not to follow the steps outlined in this procedure.

SECTION VII: Software Installation and Use

The Information Technology Department may grant specific exceptions to this policy based on organizational needs and resources. The installation of any software on any Town computer, server, or other computing device shall be performed by Information Technology Department staff. This is necessary to ensure appropriate configuration of the software, protection from malware, and proper software licensing. The technology support staff will install only licensed copies of application software within the network environment. Employees are personally responsible for violations of software licensing provisions. Reproduction of copyrighted software will not be performed without appropriate source license documentation and permission.

SECTION VIII: Use of Equipment in a Motor Vehicle

It is both hazardous and illegal to talk on a cellular telephone while operating a motor vehicle without a hands-free device. Town employees are directed that they are, under no circumstances, to use cellular telephones without utilizing a hands-free device while operating a Town vehicle or while operating any vehicle on official Town business. Note that this prohibition does not apply to those employees who are exempt by statute from the prohibition on using a cell phone in a motor vehicle. In addition, use of cellular telephones with a hands-free device should be kept to a minimum while operating a vehicle on official Town business or while operating a Town vehicle.

SECTION IX: Personal Use

Personal use of Town equipment and/or communications technology is permitted by employees who are authorized by their Department Head for use in any of the following situations:

- Performs Town related work from home
- Performs Town related work while engaged in travel away from Town facilities

The use of Town equipment in these circumstances must not be subjected to unusual wear or performance in degrading conditions not normally part of the employee’s work involving the equipment.

SECTION X: Rules for Computer Use

The following rules have been designed for proper use of Town owned computers, electronic communications, and internet access systems.

1. The electronic communications system hardware is Town property. Additionally, all messages composed, sent, received, or stored using the electronic mail system is and will remain property of the Town and will be publicly available subject to the Connecticut Freedom of Information Act except as excluded therein. These messages are not private property of any employee and the confidentiality of any message should not be assumed.

2. Town computers, electronic communications, and internet access systems shall not be used for transmitting or receiving messages that violate the Town's policies prohibiting sexual harassment or workplace violence. Attempting to or successfully sending any message anonymously where identification is required is a violation of this policy. Receipt of any messages violating these policies, shall be reported immediately by the recipient to his/her department head who in turn will report this to the Director of Human Resources.

3. In correlation with the Town of Suffield's Policy on Sexual Harassment in the Workplace, any site that displays pornography or nudity shall not be accessed. Attempting to circumvent prohibitions is a violation of this policy. Sites that are offensive or discriminatory based on race, gender, religion, national origin, or any other protected classifications of persons shall not be accessed by Town employees unless they are accessed as part of a police investigation, or authorized in advance by the Chief of Police or his/her designee.

4. Any employee who visits a site by accident that is prohibited under this policy shall forward the web site address to his or her supervisor and then to the Information Technology Department in order to repair logging effects from the site.

5. Violating any Federal, State, or local Law (including all copyright laws) is prohibited.

6. Vandalizing any hardware, software, computer, electronic communications or internet access devices is prohibited.

7. The Town system shall not be used for union business, other than by the Human Resources Department and Union officials communicating with the Human Resources Department except where the Town and Union officials agree on the said use of the system.

8. Hacking, cracking, or otherwise penetrating any hardware, software, computer, electronic communications or internet access device is strictly prohibited regardless of motivation or damage. Testing the system's security shall be the responsibility of the Town's Information Technology Department and such testing shall only be conducted under the express authorization of the Director of Information Technology.

9. Employees shall not tell anyone their password. Passwords should not be recorded where they may be found. Employees shall not use anyone else's password. Attempting to access and/or

use another person's password is strictly prohibited. The creation of additional unauthorized passwords or user identifications is strictly prohibited. The exception to this rule would be when a known Information Technology staff member is troubleshooting a problem with an employee on his or her computer.

10. Employees should not write anything about anyone that is inflammatory or defamatory. There should not be an expectation of privacy with respect to the use of the computer. E-mail is not confidential. Your e-mail and stored files are property of the Town and subject to disclosure to the public pursuant to the Connecticut Freedom of Information Act. If you do not want an email read publicly, do not write it.

11. The system is reserved solely for the conduct of business of the Town. It may not be used to solicit or proselytize commercial activity, religious or political causes, or the interest of outside organizations. Town systems may not be used for conducting private business activities except at public access network points. The system shall not be used for fundraising activities.

12. Broadcast of network wide non-business related e-mails is prohibited.

13. Privately owned computer systems, laptop computers or peripherals may only be added to the Town system with prior authorization from the Department Head and the Director of Information Technology except in designated areas intended for public access.

14. Use of Equipment may also be subject to further limitations as additional policies are adopted.

SECTION XI: Monitoring of Computer/Communications Activity

Internet (including all web sites visited), e-mail and use of computers may be monitored for compliance with this policy in accordance with the Connecticut General Statutes Sec. 31-48d[1], and as stated in Public Act No. 98-142, An Act Requiring Notice to Employees of Electronic Monitoring by Employers[2]. All messages sent over the Town computer, electronic communications, and internet access systems are the property of the Town. The Town reserves the right to review, audit, intercept access, and disclose all messages created, received, or sent over the electronic mail system for any purpose. The contents of electronic mail properly obtained for legitimate business purposes may be disclosed within the Town without permission from the employee.

SECTION XII: Records Retention

Retention of e-mail shall be described in General Letter 2009-2 (replaces GL 98-1) dated June 1, 1998, or amended, from the State of Connecticut Public Records Administrator [3].

Introduction
The Office of the Public Records Administrator and State Archives issues this statement under Authority granted by Sections 11-8, 11-8a, and 7-109 of the **Connecticut General Statutes**.

Definitions
E-mail is a means of sending messages between computers using a computer network. This

information consists primarily of messages, but may also include attachments such as calendars, directories, distribution lists, word-processing documents, spreadsheets, and other electronic documents or files. E-mail is stored in a digital format rather than on paper and is retrievable at a future date. Due to format, e-mail permits near-instant communication and transmission of up-to-date information similar to the telephone. In addition, with each e-mail sent, a record of the transmitted information is created.

Retention Guidelines
E-mail messages sent and received by public officials fall within three broad categories:

- Transitory messages, including copies posted to several persons and casual routine communications similar to telephone conversations
- Public Records with a less-than-permanent retention period
- Public Records with a permanent or permanent/archival retention period

Retention guidelines for each of these categories are as follows:

- **Transitory messages – No retention required**
  Public officials and employees receiving such communications may delete them immediately without obtaining approval from the Office of Public Records Administration and State Archives.

- **Less-than-permanent – Retention period for equivalent hard copy records applies**
  Follow retention period for equivalent hard copy records as specified in an approved retention schedule. The record must be in hard copy or electronic format that can be retrieved and interpreted for the legal retention period. When there is a doubt in the ability to retrieve an electronic record over the life span of that record, the record should be printed out or otherwise converted to its hard copy equivalent. **Municipalities and state-agency officials may delete or destroy the records only after receiving signed approval from the Office of the Public Records Administrator.**

- **Permanent or Permanent/Archival**
  Retention may be in the form of a hard copy printout or microfilm which meets microfilm standards issued in GL 96-2[4]. This information must be eye readable without interpretation.

SECTION XIII: Requirements to Access the Town Network or a Town Workstation Remotely

All users who access the Town network or a Town workstation remotely are subject to the requirements outlined within this section regardless of whether or not the user is making the connection through a town-issued or personal device. Employees using personal computers including but not limited to laptops, desktops, tablets, or phones shall be required to bring the device to the Information Technology Department to have it checked for security guideline adherence prior to configuring the device for remote access to the Town network or a Town workstation remotely.

Personal and Town-issued devices intended for remote access shall be checked for the following criteria prior to issuance:

- Up-to-date antivirus and anti-malware software

- Automatic updates enabled and up-to-date operating system software; this includes ensuring the operating system of the device is still actively receiving security updates from the creator of the operating system or the original equipment manufacturer (OEM)

- The computer must be free of viruses, malware, or other infections resulting in a potentially compromised state of security in relation to the device, the Town's network, or any other aforementioned electronics communications devices

While remotely connected to the Town network, regardless of whether or not the employee is using a personal or Town-issued device, the employee shall abide by all computer use, security practices, and/or operational standards outlined in this document.

SECTION XIV: Submitting a Support Ticket

In the event of an issue requiring intervention by the Information Technology Department, an employee shall be required to submit a Support Ticket. Support Tickets allow the Information Technology Department to catalog issues and record information related to issues including but not limited to effective procedures, required assets, and other troubleshooting information that may be of value during future issues of similar scope. Careful analysis of support ticket data allows the Information Technology Department to solve issues at an expedited rate as well as prevent future issues from occurring. As a result, it is imperative that employees submit these tickets for the benefit of everyone involved.

Guidelines for Requesting Support

- Be specific. Provide as much information directly related to the issue as possible to maximize the Information Technology Department's ability to resolve the issue.

- Identify your problem by asking yourself the following questions:
    - **Who** does this problem affect?
    - **What** happened? **What** was I doing right before the problem start? **What** is supposed to be happening that isn't?
    - **When** did the problem start occurring? **When** has this happened before? Does it happen frequently?
    - **Why** do you need this problem fixed? **What** role does the function play in your workday?
    - **How** can we fix it? **How** quickly does the issue need to be fixed? **How** did this happen?

- Give a short summary of your issue in the subject line of your e-mail.

- Carbon copy anyone this issue directly affects.

- Write an e-mail with well-thought-out answers to the above questions addressed to support@suffieldct.gov

- Remember, if everything is high priority, nothing is high priority.

SECTION XV: Violations of Policies

Any violation of any of the provisions of this policy can lead to loss of computer services, and/or progress disciplinary action, up to and including termination. Such action will depend upon the severity of the violations, the frequency of the violations, and the effect such violation has on the network or the Town.

[1] https://www.ctdol.state.ct.us/wgwkstnd/laws-regs/statute31-48d.htm

[2] http://das.ct.gov/HR/Regs/Current/State_Electronic_Monitoring_Notice.pdf

[3] http://ctstatelibrary.org/wp-content/uploads/2015/05/GL2009-2-EmailManagement.pdf

[4] https://ctstatelibrary.org/wp-content/uploads/2015/05/GL-96-2.pdf