Adopted – 05-05-99
Amended – 08-13
Amended – 05-15

# CITY OF STAMFORD TECHNOLOGY POLICY

**The City of Stamford provides information technology resources to a large and varied group, including City and Board of Education employees, elected and appointed officials, vendors, contractors, volunteers, and guests. All members of this community are accountable for using these resources in an ethical and respectful manner that protects sensitive City information and follows the information technology policies and procedures.**

**Purpose:** To establish a policy regarding the proper use of all City computer hardware, software, internal and external storage devices, electronic and other telecommunication technology systems, including but not limited to, internet, intranet, satellite, broadband, cable and similar platforms, (collectively the "Technology Systems") of the City of Stamford, Connecticut (the "City") by City and BOE employees, elected or appointed officers, contractors, consultants, and any other person or entity authorized by the City to use the Technology Systems (hereafter referred to as a "Users").

**Policy:** The following policies define appropriate use of the City of Stamford computer networks, computers, mobile devices, all related peripherals, software, electronic communications, and internet access. These policies apply to the access of the City's computer network and use of computing technology resources at any location, from any device, via wired or wireless connection. They apply to all Users of City technology resources. All Users of City computing and network resources shall use such resources in an ethical, legal, and responsible manner. All use of technology resources must be consistent with the intent and requirements of all City policies and work rules, as well as Federal and State laws. Technology resources are intended for City business purposes and may <u>not</u> be used for other commercial purposes.

The City owns all data, files, information, and communications created, stored, transmitted, received or exchanged on its network, communication systems, equipment and devices, including e-mail, voicemail, text messages and internet usage logs even if such communications reside with a third party provider. City systems and all information contained thereon are City property. Information created, sent, received, accessed or stored using the City systems is the property of the City.

The City has the right to inspect, monitor, intercept, restrict, filter, and evaluate any and all usage of the City's Technology Systems as permitted by law. No User has any right or expectation of privacy in anything that is created, sent, received or stored on or by computer (including e-mail), facsimile, cell phone (including text messages) or voice mail.

The City may conduct random and requested audits of Users' accounts (including accounts with commercial or other third party providers if used in the course of conducting City business) in order to ensure compliance with policies and requirements. Internet, e-mail, voicemail, text message communications and internet usage logs may be subject to public disclosure. Information stored, created, sent or received on City systems may be accessible under the Freedom of Information Act. Pursuant to Public Act 98-142 and the State of Connecticut's "Electronic Monitoring Notice" the State reserves the right to monitor and/or log all activities without notice. This includes but is not limited to correspondence by e-mail and facsimile.

1. Technology resources may be used for incidental personal needs as long as such use is de minimis and does not subject the city to additional cost or liability, interfere with business, productivity and/or performance, pose risk to security, cause damage to the City's reputation or credibility, or conflict with the requirements of any City policy or work rule. Professional judgment, etiquette, and common sense should be exercised while using City resources.

2. Usage should be focused on business-related tasks. Incidental personal use is allowed as discussed under the previous section, but there is no right to privacy in an employee's use of the internet. Employee internet usage is monitored. Web Usage Reports are provided to IT to help IT monitor the staff's use of the internet.

3. Except for City business-related purposes, visiting or otherwise accessing the following types of sites is prohibited:

- "Adult" or sexually-oriented web sites
- Sites associated with hate crimes or violence
- Sites associated with discrimination (racial, sexual, etc.)
- Personal dating sites
- Gambling sites
- Sites that would create discomfort to a reasonable person in the workplace

4. The City recognizes that public internet communications technologies are effective tools to promote community and government interaction and that Users may want to participate in public communication via blogging, discussion forums, wikis, mashups, social networking, message boards, e-mail groups and other media that are now commonplace tools by which people share ideas and information.

Since activities on public internet communication sites are electronically associated with City network addresses and accounts that can be easily traced back to the City of Stamford, the following rules must be followed for participation in these interactive public communication platforms.

a. When expressing User's personal view, make it clear beyond a doubt that the User's view does not necessarily represent the views of the City of Stamford. Opinions or views other than those reflective of City policy must contain the following disclaimer: "The opinions expressed in this communication are those of the author and not the opinions of the City Government or management, nor are the opinions endorsed and/or encouraged in any way by the City of Stamford."
b. Always protect the confidentiality, integrity, and availability of all critical information.
c. Users may not post any material that is obscene, profane, threatening, harassing, abusive, hateful, or embarrassing to or of any other employee, person, and/or entity.
d. Public internet communications activity should contribute to staff's body of work as an employee of the City and may not interfere with or diminish productivity.

5. E-mail content must conform to the standards that apply to any other form of written (or verbal) communication occurring in a business setting and to documents that are subject to public disclosure.

6. The City provides Users access to Exchange/Outlook messaging (email) system. Access or usage of any other messaging systems for personal use is permitted. However, such usage will not be supported by the City IT department. Staff may access web-based personal email but should not download personal documents or attachments from these sites. Staff may not install client based software such as AOL for internet service on city equipment.

7. Users should be observant of e-mails that have unusual or questionable subject lines to avoid or mitigate spam, phishing and script born viruses that come into the network through email attachments or by clicking on links that lead to hostile/inappropriate web sites. Upon discovery, Users should report suspicious emails to the IT Department.

8. Users shall not use the City's Technology Systems, including access to the internet, to disseminate indecent information, material, images or messages including, but not limited to, sexual innuendo, chain letters, jokes, harassing or threatening statements. Additionally, Users shall not disseminate information, material or messages, which may be hostile or offensive to another based on sex, age, race, religion, color, national origin, sexual orientation, marital/civil union status or disability. Indecent, vulgar, harassing, fraudulent, intimidating or other unlawful material may not be sent by e-mail, voice mail, facsimile or other form of electronic communication, or displayed on or stored in the City's Technology Systems except by law enforcement officials during official investigations.

While Users cannot always control what material they receive, Users who do receive any such referenced material from any other User or third party must <u>not</u> transmit or forward such material to any other person. The recipient User should request the sender to stop sending the User inappropriate material.

9. The use of e-mail to send or solicit the receipt of inappropriate content such as sexually oriented materials, hate mail, content that a reasonable person would view as obscene, harassing or threatening and having no legitimate or lawful purpose or any other inappropriate content is prohibited.

10. The incidental personal use of e-mail from a City account to express opinions or views other than those reflective of City policy must contain the following disclaimer: "The opinions expressed in this communication are those of the author and not the opinions of the City Government or management, nor are the opinions endorsed and/or encouraged in any way by the City of Stamford."

11. The City has an obligation to retain certain information stored on the Technology Systems in accordance with General Letter 98-1 "Electronic and Voice Mail: A Management and Retention Guide for State and Municipal Government Agencies" issued by the State of Connecticut Office of Public Records Administrator and State Archives as it may be amended from time to time. While many e-mail messages are temporary communications which are non-vital and may be routinely discarded, email messages that are more formal or substantive must be retained by the City in accordance with state standards. Examples of such messages include, but are not limited to, messages related to policies, decision-making, material connected to a specific case or business matter, contracts, parts of a larger record, or business functions.

12. The IT Department must authorize access to central computer systems. The use of another User's account is prohibited. Users are responsible for protecting access to the network by locking their computers or logging out of their accounts when leaving their computers unattended. Staff members with access to critical information are responsible for its protection. Staff must, to the best of their ability, ensure the safety of critical information by, for example, not putting important information on laptops, not storing, saving, or transmitting critical data to a home computer or other personal devices.

13. Users should not transport critical City data on unencrypted devices such as thumb drives, CD's, or Smartphones.

14. Users are prohibited from sharing their passwords or allowing anyone else to use their network accounts for any reason. It is the User's responsibility to protect his/her password and access to the network.

15. Users are not permitted to directly connect devices to the City/BOE network. This includes PC's, network hubs and switches, printers, scanners, handheld devices as well as wired and wireless devices.

16. The installation, removal, copying, or altering of any software on City-owned equipment is prohibited without authorization.

Users must comply with all software licenses, copyrights, and all other laws governing intellectual property, including all materials found on the internet.

17. Disabling, altering, over-riding, or turning off any mechanism put in place for network protection is forbidden. This includes the installation of any software designed to circumvent security measures.

18. Any technology resource found to be lost or stolen should be immediately reported to the Technology Department and the Risk Management department. If technology is stolen, a police report will be required.

19. The City may acquire and place wireless Technology (such as Cell Phones, Smart Phones and Tablets) into service in those instances where such technology will enhance the ability of City Users: to deliver services more effectively and/or to protect or otherwise secure public safety and well-being.

> The approval of a request for a cellular device must be made, by the employee's Director, before the department may proceed to purchase equipment and service. All purchases of cellular devices and services will be made through the vendor selected by the City.
>
> Like all other City assets, technology and resources, the use of mobile devices is also subject to review at the discretion of the City. City employees are responsible for calls placed and received on the devices assigned to them.

20. Please consult with the IT department prior to purchase as not all devices are compatible with the City/BOE network.

Each User is responsible for using the City's Technology Systems, resources and services in an efficient, effective, ethical and lawful manner and in accordance with applicable statutes, ordinances and this Policy. This Policy applies to all Users of the City's Technology Systems, wherever the Users or Technology Systems are located. Violations of this Policy will not be tolerated and may result in disciplinary action up to and including termination. Non-employee Users who violate this policy may have their right to access to or use of the City's Technology Systems revoked.

The City reserves the right to monitor its Technology Systems at any time, without notice, to ensure they are being used for City purposes only. The City's monitoring policy will be in accordance with all applicable federal and state laws, including Public Act 98-142 (codified at Conn. Gen. Stat. Sec. 31-48d).

This policy may be amended or revised from time to time at the City's discretion.