



CITY OF NORWALK TECHNOLOGY POLICY

PURPOSE: To establish a Policy for the acceptable use of the computer, electronic and telecommunication technology systems and services (collectively the "Technology Systems") of the City of Norwalk (the "City") by each City officer, employee, contractor, consultant or any other person or entity authorized by the City to use the Technology Systems (hereafter referred to as a "User").

POLICY: The City's Technology Systems, including but not limited to E-mail, voice mail and internet are City property and are intended for City business purposes, and may not be used for other commercial purposes. Incidental, de minimis personal use of the Technology Systems that is not inconsistent with this policy is permitted. Any such personal use must be occasional, during breaks or non-work time, shall not interfere with the User's performance of his or her job duties or City operations, or consume significant Technology System resources.

The City has the right to 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 by computer (including E-mail), fax, cell phone (including text messages) or voice mail.

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 or use of the City's Technology Systems revoked.

More specifically, the following rules apply to the use of the City's Technology Systems:

1. Users must comply with all software licenses, copyrights, and all other laws governing intellectual property, including all materials found on the Internet.
2. The City's Technology Systems, including access to networks, shall be used by Users in connection with the recognized public purposes of the City and shall not be used for the transmission or storage of private advertisements, solicitations, promotions, destructive programs (viruses and/or self replicating codes), internet remote control software and political material or for any unauthorized use.

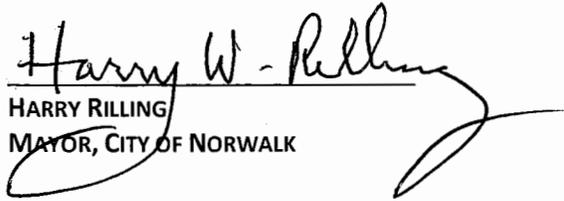
3. Users shall not use the City's Technology Systems, including access to the Internet, to disseminate indecent information, material, images or messages including, but not limited to, sexual innuendo, chain letters, jokes, harassing or threatening statements. Additionally, Users shall not disseminate information, material or messages which may be hostile or offensive to another on the basis of 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, fax 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 not transmit or forward such material to any other person.

4. Users should use the same care in drafting E-mail and other electronic documents as they would for any written communication. Except as permitted or required by law, anything transmitted electronically, by facsimile or E-mail, is not confidential, and may be reviewed by others.
5. Users may not install software in their individual computers or the network without first receiving express written authorization to do so from the Director of Information Services. Any software that is not properly licensed may be deleted or removed without notice.
6. E-mail messages dealing with legal issues sent to or by any employee in the Office of Corporation Counsel must include a header on each page containing material which should remain confidential that reads as follows: "Privileged attorney-client communication. Do not forward unless authorized." Said emails may be forwarded to other employees who are on a "need to know" basis without prior authorization.
7. No E-mail message, written document or other communication originating from or addressed to the Corporation Counsel to any employee or officer of the City may be disclosed, disseminated or distributed to any person or persons without the express written authorization of the Corporation Counsel.
8. Users will be issued a standard User identification by the Information Technology Department which identification is to be used only by that User. An initial password will be assigned to that identification by the Information Technology Department and must be changed when the User first logs on to the network. Users should regularly change their password for security purposes. Users are responsible for safeguarding their passwords for any and all of the Technology Systems. Individual passwords should not be printed, stored online or shared with others unless required for support by authorized IT staff. Users are responsible for all transactions made using their passwords.

9. A User's ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.
10. Access to and use of the Internet is restricted to business use of the City, by authorized Users except as otherwise permitted herein. A User's Internet activities may be logged by a surveillance system and reviewed by authorized City personnel. Users who use the Internet for indecent, vulgar, harassing, fraudulent, intimidating or other unlawful purposes, or who visit web sites that contain such material, are subject to discipline, up to and including termination and for non-employee users revocation of their access and/or use of the Systems.
11. Information or electronic communications using the City's Technology Systems are subject to release pursuant to the Freedom of Information Act of the State of Connecticut and may also be subject to disclosure in legal proceedings.
12. 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 the 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, E-mail 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, part of a larger record, or business functions.
13. Users who are uncertain whether a specific E-mail message must be retained should err on the side of caution and retain it. Users should be aware, however, that when they have deleted a message from their mailbox, it may not have been deleted from the E-mail system's back-up function.
14. Broadcast email messages must be pre-approved by the Personnel department in writing for mass distribution.
15. Any User who (a) misuses or abuses the Technology Systems of the City, (b) violates this Policy, (c) violates the law or the legal rights of the City or any City employee by utilization of the Technology Systems of the City, or (d) creates a hostile work environment by utilization of the Technology Systems of the City, is subject to discipline, up to and including termination. Pursuant to Connecticut law, the City may use electronic monitoring as evidence of a User's misconduct.
16. The City reserves the right to monitor its Technology Systems at any time, without notice, to ensure they are being used in accordance with this policy. 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), a copy of which is attached to this Policy.

17. Employees with questions regarding this Policy should contact their Director or Director of Personnel for clarification.
18. This Policy may be amended or revised from time to time at the City's discretion.


HARRY RILLING
MAYOR, CITY OF NORWALK

ACKNOWLEDGEMENT

I acknowledge that the City has provided me with the City's Technology policy and Surveillance notice required under Public Act 98-142 (codified at Conn. Gen. Stat. Sec. 31-48d) indicating that it may monitor my use of its Technology systems. I have read and understand the above policy and attached notice.

Signature

Print Name

Date



THE CITY OF NORWALK SURVEILLANCE NOTICE

Pursuant to the authority of Public Act 98-142, (codified at Conn. Gen. Stat. Sec. 31-48d) the City of Norwalk hereby gives notice to all its employees of the potential use of electronic monitoring in its workplace. While the City may not actually engage in the use of electronic monitoring, it reserves the right to do so when determined by the City.

“Electronic monitoring,” as defined by Public Act 98-142, means the collection of information on the City’s premises concerning employees’ activities or communications, by any means other than direct observation of the employees. Electronic monitoring includes the use of a computer, telephone, cell phone wire, radio, camera, electromagnetic, photo electronic or photo-optical systems. The law does not cover the collection of information (A) for security purposes in any common areas of the City premises which are open to the public, or (B) which is prohibited under other state or federal law.

The following are some types of electronic monitoring that may be used by the City in its workplace:

- Monitoring of e-mail and other components of the City’s technology systems for compliance with policies
- Video surveillance of employee parking areas for security purposes or to insure compliance with policies or performance standards
- Telephone monitoring (customer service only) for quality control and performance assessment
- Monitoring of electromagnetic card access system for security purposes

The law also provides that, where electronic monitoring may produce evidence of misconduct, the City may use electronic monitoring without any prior notice when the City has reasonable grounds to believe employees are engaged in conduct that (i) violates the law, (ii) violates the legal rights of the City or other employees, or (iii) creates a hostile work environment.

Questions about electronic monitoring in the workplace should be directed to H. James Haselkamp, Jr., Director of Personnel, City of Norwalk (203)-854-7724.