PAUL J. FETHERSTON
TOWN MANAGER

TOWN OF NEWINGTON

131 CEDAR STREET
NEWINGTON, CONNECTICUT 06111

OFFICE OF THE TOWN MANAGER

Information Technology Policy
Effective Immediately
February 1, 2005

SUBJECT : Acceptable Use Policy

PURPOSE : To establish an Acceptable Use policy that outlines the appropriate use of communications equipment (data/ voice) owned by the Town of Newington (hereinafter "Town") and to establish guidelines and procedures with regards to use of the Town's communication networks.

The Town, committed to protecting Town employees and the Town from knowingly or unknowingly engaging in illegal or damaging actions by individuals, prohibits inappropriate uses which expose the Town to risks including virus attacks, the compromise of network systems and services, and other legal issues. Services, equipment and systems including but not limited to telephone, paging, faxing, Internet, Intranet, Extranet, FTP, Telnet related systems, computers, software, operating systems, storage media, network accounts providing electronic mail, WWW/HTTP browsing are the property of Town. These systems shall be used for business purposes in serving the interests of the Town, its citizens and customers in the course of normal operations. Effective security requires the participation and support of all Town employees, its agents and affiliates who deal with information and/or data and voice systems. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

APPLICABILITY: This policy applies to all Town employees, its contractors, vendors, consultants, agents, and affiliates, including all personnel affiliated with third parties. This policy also applies to all equipment owned, leased, and/or utilized to access the Town's communication networks.

1.0 General Use and Ownership

1.1. While the Town desires to provide a reasonable level of privacy, users should be aware that all data, applications, including code, created on Town systems and/ or Town time remains the property of the Town. The Town does not guarantee the confidentiality of information stored on any device belonging to the Town or any device used to access the Town's networks.

1.2. Employees shall exercise good judgment in using the Town's communication networks in the performance of their assigned duties.

1.3. For security and network maintenance purposes, the Town Manager and/ or his/ her duly authorized designee may monitor equipment, systems and network traffic at any time in accordance with the Town's Acceptable Use Policy and Audit Policy.

1.4. The Town reserves the right to audit its communication networks and systems on a periodic basis to ensure compliance with this policy.

1.5. No person(s), other than Town Information Systems and Technology (hereinafter "IST") staff and its duly authorized agents, may install and/ or uninstall software and/ or make any hardware/ software modifications to computers and communications equipment operated by the Town.

1.6. No person(s), other than authorized IST staff and/ or its duly authorized agents may connect any equipment to the Town's communication networks (i.e. connection of personal computers or unauthorized equipment onto Town communication networks.)

1.7. All software used on the Town communication networks shall be registered to the Town of Newington (Company Name) with a user name of Newington (Last Name) and Town of (First Name).

Phone: (860) 665-8510 Fax: (860) 665-8507
townmanager@ci.newington.ct.us
www.ci.newington.ct.us

2.0 Security

2.1. Authorized users are responsible for the security of their passwords and accounts. Passwords and accounts should not be shared. System level passwords should be changed quarterly, while user level passwords shall be changed every ninety (90) days. Any user who suspects that his/her network account has been compromised SHALL notify IST immediately after changing their password in accordance with the Town's Password Policy.

2.2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the host will be unattended. In the case of sensitive material user shall activate security if they need to leave computer unattended.

2.3. Since information contained on portable computers is especially vulnerable, special care should be exercised to ensure the physical security of these devices.

2.4. Unless performed in the course of professional business duties no employee shall post to newsgroups from a Town affiliated email address without the express permission of the Town Manager and/ or his/her duly authorized designee. Any authorized posting shall contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Town.

2.5. Unless expressly authorized in writing by the Town Manager and/ or his/ her duly authorized designee, all hosts used to connect to the Town's communication networks via Internet/Intranet/Extranet, shall be continually executing approved virus-scanning software with a current virus database and running an approved firewall application/device.

2.6. Employees shall exercise extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code, in accordance with the Town's E-mail Policy.

3.0 Unacceptable Use

3.1. Definition

3.2. Unless expressly authorized by the Town Manager and/ or his/ her duly authorized designee, employees are prohibited from engaging in the following activities. Exceptions to this policy shall be limited to activities necessitated to complete legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

3.3. Under no circumstances is an employee of the Town authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Town resources.

3.4. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.0 System and Network Activities

The following activities are strictly prohibited, unless overridden in writing by the Town Manager and/ or his/her duly authorized designee:

4.1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Town.

4.2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Town or the end user does not have an active license is strictly prohibited.

4.3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The Town Manager and/ or his/ her duly authorized designee shall be consulted prior to export of any material that is in question.

4.4. Introduction of malicious programs into the Town's communication networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.5. Revealing your account password to others or allowing use of your account by others. This includes but is not limited to temporary employees, town employees, vendors and family or other household members when work is being done at home.

4.6. Using a Town computing asset to actively engage in procuring or transmitting material that is in violation of laws and Town policies pertaining to sexual harassment or hostile workplace.

4.7. Making fraudulent offers of products, items, or services originating from any Town account.

4.8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server/workstation or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.10. Port scanning or security scanning is expressly prohibited except by the Town's Director of Information Systems and Technology and/ or his/ her duly authorized agents.

4.11. Executing any form of network monitoring which will intercept data not intended for the employee's host, except by the Town's Director of Information Systems and Technology and/ or his/ her duly authorized agents.

4.12. Circumventing user authentication or security of any host, network or account.

4.13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

4.14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.15. Providing information about, or lists of, Town employees to parties outside the Town organization.

4.16. Connection of any personal computers, laptops, handheld computers, PDAs or networking equipment onto any portion of the Town's communication networks without written authorization from the Town Manager and/ or his/ her duly authorized designee.

4.17. Connection of PDA's (Personal Digital Assistants) including but not limited to Palm, Visor and PocketPC to Town owned/ leased equipment. Per the Town Manager, Town Department Heads are exempt from this restriction but only the Outlook/Exchange connector will be configured to sync email, contacts and calendar.

4.18. Peer to Peer software including but not limited to: Kazza, Morpheous, LimeWire, etc.

4.19. Playing of computer games including but not limited to: (Solitaire, Hearts, Online gaming, etc.)

5.0 Email and Communications Activities

The following activities are strictly prohibited, unless overridden in writing by the Town Manager and/ or his/her duly authorized designee:

5.1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

5.2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

5.3. Unauthorized use, or forging, of email header information.

5.4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5.5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

5.6. Use of unsolicited email originating from within the Town's communication networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Town or connected via the Town's communication networks.

5.7. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).
5.8. Access to POP/ Web based email.
5.9. Use of Instant Messaging including but not limited to: AOL, Yahoo, MSN, etc.

6.0 Exceptions

Exceptions to the Town's Acceptable Use Policy and/ or any policies covering the Town's communication networks are handled on a case by case basis. Exceptions must be submitted in writing to the Town Manager and/ or his/ her duly authorized designee. Copies of any exception requests will be maintained on file.

7.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8.0 Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.
Host	Computer, laptop, PDA, or device used to access Town's communication networks.
Ponzi	Pyramid scheme
Trojan Horse	A program that appears desirable but actually contains something harmful; "the contents of a trojan can be a virus or a worm"; "when he downloaded the free game it turned out to be a trojan horse"
Email Bomb	Computer software (computer programs) whose express purpose is to cause harm. Computer viruses, computer worms, Trojan horse programs and logic bombs are all examples of malware or malicious software.
Virus	(Computers) a program or segment of program code that may make copies of itself (replicate), attach itself to other programs, and perform unwanted actions within a computer; also called computer virus or virus program. Such programs are almost always introduced into a computer without the knowledge or assent of its owner, and are often malicious, causing destructive actions such as erasing data on disk, but sometime only annoying, causing peculiar objects to appear on the display.
Firewall	A computer or computer software that prevents unauthorized access to private data (as on a company's local area network or intranet) by outside computer users (as of the Internet)
Networking Equipment	Including but not limited to computers, laptops, servers, facsimile machines, printers, card readers, USB or IEEE Firewire devices.

_____
Paul J. Fetherston
Town Manager