

***Town of Belmont******Electronic Communications  
And  
Computer Usage Policy***

<i>Creation Date: 10/01/2007</i>	<i>Title: Electronic Communications and Computer Usage Policy</i>
<i>Approval Date: 12/15/2008</i>	<i>Approval Authority: Board of Selectmen</i>
<i>Effective Date:</i>	<i>Policy Number: 005</i>
<i>Reviewed Date: 12/14/2008</i>	<i>Final: 12/14/2008</i>

**I. Purpose**

This Policy is intended to provide guidance on the appropriate use of the Town of Belmont's electronic communications and information equipment and systems ("Systems") including, but not limited to, Computer Workstations, Hardware and Software, Electronic Mail ("e-mail"), Internet, Printers, Plotters, Scanners, Personal Digital Assistants (PDA's), Cameras, Facsimile Machines (FAX), Copiers, LCD Projectors, and Network Devices such as Switches, Hubs, and Wireless Access Points.

**II. Scope**

Use of the Town of Belmont's Systems by any employee, contractor, consultant, volunteer, intern or any other person so authorized including, but not limited to, any part-time, full-time, elected or appointed personnel ("user") shall constitute acceptance of the terms of this Policy and any such additional related policies that may be issued by the Town of Belmont.

### **III. Policy**

Users shall use the Town of Belmont's Systems in a responsible, professional, ethical, and lawful manner. Access and use of the Town of Belmont's Systems is intended for business-related purposes, including communicating with co-workers and colleagues, and researching topics relevant to Town of Belmont business. All existing state, federal, and local laws and Town of Belmont policies apply to your conduct while using the Town of Belmont's Systems, particularly those that govern intellectual property protection, sexual or other harassment, misuse of Town of Belmont resources, privacy rights, and confidentiality.

This Policy sets forth general guidelines and examples of prohibited uses of the Town of Belmont's Systems for illustrative purposes, but does not attempt to identify all required or prohibited activities by users. Questions regarding whether a particular type of activity or use is acceptable should be directed to the Information Technology Manager and/or your supervisor. These guidelines may be supplemented by more specific administrative procedures and rules governing day-to-day management and operation of the Town of Belmont's Systems. Furthermore, this Policy may be amended from time to time and is meant to be read in conjunction with all other applicable policies of the Town of Belmont.

### **IV. Review**

This Policy will be reviewed by the Information Technology Manager and the Town Administrator, or any person so designated by the Town Administrator, on a period basis to ensure that it is legally sound and reasonably enforceable.

### **V. Training and Notification**

Users shall become familiar with, and adhere to, the provisions of this Policy and receive in-service training at time of hire and periodically thereafter, as necessary. In addition, users will receive notifications pertaining to this Policy by internal mail, email, bulletin board posting, and occasional network log-on reminders.

### **VI. Privacy**

Users should not expect any right of privacy in the Town of Belmont's Systems, including electronic communications and information created or stored on the Town of Belmont's Systems. The Town of Belmont retains the right to inspect all data files, electronic information, data created and/or communicated to and from users of the Town of Belmont's Systems. Said communications may also be subject to audit checks, security assessments, and forensic examinations. Users should be aware that appropriately authorized network administrators may monitor network traffic, and/or access all files, including e-mail files and Internet use history, stored on any Systems. The Town of Belmont, in order to ensure the continuity and safe operations of its Systems, may employ intercept, capture, and/or detection programs that search for patterns of abuse, security risks, illegal activity, and any violation of this Policy.

All electronic files and documents originating from or passing through the Town of Belmont's Systems are considered to be the property of the Town of Belmont.

## VII. Security

- A. Users shall restrict access (electronically and/or physically) to their Systems to ensure adequate security and prevent destruction or tampering with the Systems. This includes computer equipment and Systems located in motor vehicles and/or any Town-owned device in the user's possession, such as a laptop or PDA.
- B. Users shall conduct a daily visual and operational inspection on all Systems, and if there appears to be any damage, tampering or malfunctioning of the Systems, this must be reported as soon as possible to the Information Technology Department.
- C. Users shall log into the department computers in their designated work areas (on a regular basis) to read and respond to official department emails. Users are required to know their email user names and passwords and are responsible for logging into and out of their accounts. Users are prohibited from giving their personal passwords to others, and/or leaving unattended, open access to their email/network accounts. Users shall not allow others to use their assigned email accounts, unless configured to do so by the Information Technology Department.

## VIII. Internet/E-mail Guidelines

While we increasingly use the Internet and E-mail as a tool in the workplace, misuse or abuse of the Internet and E-mail can result in wasted time, as well as potentially violate laws, bylaws, ordinances, regulations or other Town of Belmont policies. Therefore, users should adhere to the following Internet and E-Mail Guidelines.

- a. **Use for Official Business.** It is the Town of Belmont's' policy to restrict Internet and E-mail access to official Town of Belmont business. Use of the Internet or E-mail for personal matters is prohibited, unless prior authorization is obtained from the users' department head. Users, upon obtaining approval from their respective department head, may use the department computer equipment, applications, programs or Systems for limited personal use, ensuring that this use does not interfere with their primary job responsibilities. Users are expected to demonstrate a sense of responsibility and not abuse this limited use privilege. The department head shall monitor personal use to determine if abuse occurs.
- b. **Authorization.** Authorization for Internet and E-mail access must be obtained through the Information Technology Manager. Once authorization is approved, each user is responsible for the security of his or her account password and will be held responsible for all use or misuse of such account.
- c. **Compliance with Laws.** Users must not utilize the Internet or E-mail to knowingly violate any state, federal or local law, or the laws of any other nation. United States copyright and patent laws may apply to information and material(s) accessed through the Internet, and care should be taken to not violate the copyrights or patents of others on or through the use of the Internet or E-mail. Users shall respect and comply with all software licensing agreements and are forbidden to use, copy, retrieve, modify or forward copyright-protected materials, except as permitted by law.

- d. **Viruses.** All appropriate precautions should be taken to detect viruses, including scanning all computer files (including attachments) that are downloaded and/or opened from the Internet, before installation or execution of such files/attachments. Users should only open attachments from anticipated and trusted sources. Users should direct any questions regarding the proper use of virus detection software to the Information Technology Department prior to downloading and/or opening any computer files/attachments
- e. **Monitoring.** As noted above, users should not have any expectation of privacy as to their computer or Internet usage, including receipt and sending of e-mail. It is possible for the Town of Belmont to monitor Internet usage histories and/or patterns, and the Town of Belmont may inspect, without limitation, any portion of its Systems, including files stored either on the computer hard drive or the Town of Belmont's server, to the extent necessary to ensure compliance with this Policy or any other applicable state, federal, or local law of Town of Belmont policy.
- f. **Public Records Law.** Users shall familiarize themselves with the Commonwealth's Public Record Laws. The Secretary of State's Office of the Commonwealth has determined that e-mail (and any attachments) qualifies as "public records," as defined in Chapter 4, section 7(26) of the Massachusetts General Laws. Therefore, all e-mail sent by or received through the Town of Belmont's Systems shall be archived by the Information Technology Department. All users shall retain either a printed or digital record of e-mail sent by or received through the Town of Belmont's System's, in the same manner that other paper records are kept by their departments, and in accordance with the Record Retention requirements.
- g. **Prohibited Practices.**
  - 1. Unless it is directly related to an approved investigative operation, users are prohibited from using the Town of Belmont's Systems, including any device connected to the Town Network VLAN or telephone dial-up lines, to knowingly display, transmit, download, receive, store, archive, distribute, edit and/or record any unlawful or offensive communication and/or computer file, that is:
    - a. Discriminatory or harassing;
    - b. Derogatory to any individual or group;
    - c. Obscene, sexually explicit, sexually suggestive or pornographic;
    - d. Defamatory or threatening;
    - e. Promotional of one's personal political beliefs;
    - f. In violation of any state or federal law, regulation, or local bylaw; or
    - g. In violation of any license governing the use of software or copyrighted material. Users shall not use the Town of Belmont's computers to knowingly download or distribute pirated software or data. Any software or files downloaded via the Internet may be used only in ways that are consistent with their licenses or copyrights. The downloading of games or other programs for amusement/entertainment (or any other personal) purposes is strictly prohibited.

2. Users are forbidden from disseminating any child pornography or other pornography to anyone by any means.
3. Unless otherwise authorized by this Policy, users are prohibited from engaging in or attempting to engage in:
  - a. Maliciously using or disrupting the Town of Belmont's computers, networks, or Internet services;
  - b. Misusing or damaging the Town of Belmont's equipment or Systems;
  - c. Monitoring or intercepting the files or electronic communications of other users or third parties;
  - d. Hacking or obtaining access to systems or accounts (internal or external), which they are not authorized to use;
  - e. Using another user's network log-in account, email address(es), and/or password(s);
  - f. Breaching, testing or monitoring a Town-owned computer or System or tampering with the Town's system configuration and/or network security measures;
  - g. Attempting to access unauthorized sites;
  - h. Using the Town of Belmont's Systems after such access has been denied or revoked;
  - i. Attempting to delete, erase or otherwise conceal any information stored on any portion of the Town of Belmont's Systems; or
  - j. Installing any software program, application or hardware device on a Town-owned computer or System without first obtaining authorization from the Information Technology Manager or his designee.
4. Users shall not (unless approved and acting in an investigative capacity) send e-mail or other electronic communications that hide the identity of the sender or represent the sender as someone else or utilize any form of spoofing, masquerading and/or anonymous relaying/WEB surfing services.
5. Users shall not use or abuse software programs, computer resources or Systems in a manner that is likely to cause major network congestion or significantly hamper the ability of other users to access and use the system or network.
6. Users shall not broadcast messages to all employees or users via e-mail without permission from their supervisor. Users shall not utilize the Town of Belmont's Systems for the purpose of sending "chain-letters, unsolicited mass e-mails, or other "spam."
7. Users shall not utilize the Internet or e-mail to deliberately propagate any virus, worm, "Trojan horse," trap-door or back-door program code, or knowingly disable or overload any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.
8. Users shall not utilize the Town of Belmont's computers or Systems for private financial gain, or commercial, advertising or solicitation purposes.

**9.** Users shall refrain from using encrypted programs and encrypted communications (unless previously approved by the Information Technology Manager). Encrypted programs may only be used for the purposes of safeguarding sensitive/confidential information and certain authorized online investigations. Users, authorized to use various forms of encryption on files and communications, must provide the Information Technology Manager with a sealed printed copy (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files, including any user accounts and passwords used in accessing secure resources and network configurations.

**10.** Users shall not store confidential information or Non-Public Information (NPI) locally on desktop or mobile computers or on any removable device or media such as floppy disks, CD's, DVD's, iPods, PDA's, cell phones, and flash/jump drives. Confidential information and NPI is defined as information that is exempt from disclosure under the Freedom of Information Act; protected by statute, Executive order, or regulation; designated by the Town as confidential; or not yet made available to the public or authorized to be made available. Examples of NPI include, but are not limited to:

- a. Social Security Numbers;
- b. Credit card or bank account numbers; or
- c. Medical or educational records.

**11.** Users shall not transmit or disclose, via email or any other means, confidential information or NPI unless it is a necessary function of the user's duties, in which case such transmission must be encrypted.


**12.** All computer hardware, software and Systems shall at all times remain the property of the Town of Belmont and shall not be removed from their respective sites or downloaded onto personal computer equipment without the express written approval of the Information Technology Department. Users shall not reassemble and/or disassemble computer equipment or Systems belonging to the Town of Belmont without express permission from the Information Technology Department.

## **IX. Violations of Policy**

Users have read, understand, and agree to comply with this Policy, governing the use of the Town of Belmont's Systems. Those individuals who violate this Policy or otherwise abuse the privileges and guidelines set forth in this Policy may be subject to corrective action including, but not limited to, possible termination of employment, legal action, and criminal liability. Additionally, users shall be personally liable for any losses, costs or damages incurred by the Town of Belmont related to violations of this Policy.

Users shall report violations of this Policy to their supervisor, or in the case of department heads, directly to the Town Administrator. Retaliation against another user for reporting a violation or violations of this Policy, including the use of e-mail or the Internet in a retaliatory manner, is strictly prohibited by the Town of Belmont.

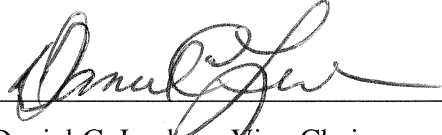
This Policy has been reviewed and approved by the Board of Selectmen:



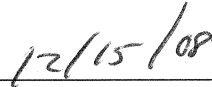
Angelo R. Firenze, Chairman



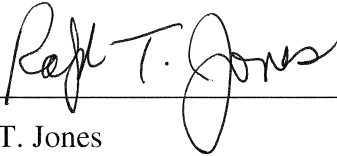
Date



Daniel C. Leclerc, Vice Chairman



Date



Ralph T. Jones



Date