



# Town of Wellesley

## Information Technology Resources (ITR) Policy

Rev. 2.3

December 13, 2013

This document formalizes the policy for all Town of Wellesley (Town) employees on the use of **information technology resources**; ("Town ITRs"), including computers, printers and other peripherals, programs, data, local area network, e-mail, and the Internet. In addition to this policy, individual departments may choose to issue supplemental policies governing their use of Town ITRs. Any person with questions regarding the application or meaning of this policy should seek clarification from the Information Technology Department (ITD).

Use of Town ITRs by any employee shall constitute acceptance of the terms of this policy and any such additional policies. It is the responsibility of any person using Town ITRs to read, understand, and follow this policy. In addition, users are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of ITRs. Failure to observe this policy may subject individuals to disciplinary action, including termination of employment.

### 1. Acceptable Uses

- Town ITRs are intended for and should be used for Town business only
- Employees are encouraged to use provided ITRs in support of Town goals and objectives
- Incidental personal use is permitted, providing it does not conflict with the security guidelines of this policy, interfere with workstation or network performance, or result in employee productivity loss
- Network accounts are to be used by the authorized owner of the account for the authorized purpose
- Applications and computers are to be logged off and shutdown at end of business day

### 2. Unacceptable Uses

- Perpetrate an illegal act, including violation of any criminal or civil laws or regulations, whether state or federal
- Use for political purpose
- Use for commercial purpose
- Send threatening or harassing messages, whether sexual or otherwise
- Access or share sexually explicit, obscene, or otherwise inappropriate materials to infringe any intellectual property rights
- Gain, or attempt to gain, unauthorized access to any computer or network
- Use that causes interference with or disruption of Town ITRs, including propagation of computer viruses or other harmful programs
- Intercept communications intended for other persons
- Misrepresent either the Town or a person's role at the Town
- Distribute chain letters
- Access online gambling sites
- Access social media sites (e.g. Facebook, Twitter, etc.)

- Libel or otherwise defame any person
- Install software or hardware not approved by ITD

### **3. Data Confidentiality**

In the course of performing their jobs, Town employees often have access to confidential or proprietary information, such as personal data about identifiable individuals or commercial information about business organizations. Under no circumstances is it permissible for employees to acquire access to confidential data unless such access is required by their jobs. Under no circumstances may employees disseminate any confidential information that they have access to, unless such dissemination is required by their jobs.

### **4. Software / Copyright Protection**

Computer programs are valuable intellectual property. Software publishers are entitled to protect their property rights from infringement. In addition to software, legal protections can also exist for any information published on the Internet, such as the text and graphics on a web site. As such, it is important that users respect the rights of intellectual property owners. Users should exercise care and judgment when copying or distributing computer programs or information that could reasonably be expected to be copyrighted.

### **5. Network Security**

Most desktop computers are connected to the Town's local area network. It is critically important that users take particular care to avoid compromising its security. All network user accounts require strong password authentication and all passwords must be established according to rules promulgated by ITD. Users should never share their passwords with anyone else, and should promptly notify ITD personnel if they suspect their passwords have been compromised. In addition, users who will be leaving their PCs unattended for extended periods should either log off the network or have a password-protected screen saver in operation. Finally, no user is allowed to access external networks or Internet-based file sharing services unless they have received specific permission from the ITD Network Manager and/or IT Director.

### **6. Computer Viruses**

ITD implements a number of industry standard measures to ensure the security of the Town's local area network (blocked internet sites, filtering of incoming / outgoing e-mail, etc), but users should still exercise reasonable precautions in order to prevent the introduction of computer viruses. Virus scanning software should be used to check any software downloaded from the Internet or obtained from any questionable source. In addition, executable files (such as program files that end in ".exe") should not be stored on or run from network drives. Finally, it is a good practice to scan removable, recordable media periodically to check if they have been infected.

### **7. E-mail**

When using e-mail, there are several points users should consider. First, because e-mail addresses identify the organization that sent the message (username@wellesleyma.gov), users should consider e-mail messages to be the equivalent of letters sent on official letterhead. For the same reason, users should ensure that all e-mails are written in a professional and courteous tone. Second, although many users regard e-mail as being similar to a telephone in offering a quick, informal way to communicate, users should remember that e-mails can be stored, copied, printed, or forwarded by recipients. As such, users

should not write anything in an e-mail message that they would not put into a memorandum. Finally, users should understand that all e-mail created or received by a Town employee is a public record and is subject to public access and disclosure through the provisions of the MA Public Records Law, MGL c.66 §10.

ITD approved versions of Microsoft Outlook are the only e-mail software permitted for use from Town computers on the local area network. Use of other webmail services (e.g. Yahoo, Gmail, Hotmail, etc) from computers on the local area network is a threat to security and strictly prohibited.

Remote access to Town e-mail functions across the Internet through Outlook Web Access (OWA) is provided to end users who have a demonstrated need to remotely retrieve their emails. Users must request, in writing, permission to use webmail from their respective department head, ITD Network Manager and/or IT Director.

## **8. Wireless Access**

Use of wireless access from Town's ITRs is strictly prohibited

## **9. Remote Access to Town ITRs**

Secure remote access software and SSL VPN ensure encrypted communications channel for data and other information between remote client computers and Town ITRs. This provides a reliable and secure remote authenticated pathway mechanism to Town ITRs.

ITD approved versions of Citrix Receiver and endpoint security compliance ensure the remote client computer complies with security prerequisites (eg, up to date anti-virus definitions, particular Windows configurations, etc.) before allowing a remote logon.

Remote access to the Town's ITRs through Citrix XenApp services is provided to end users who have a demonstrated need to remotely connect to network resources and applications in order to perform their job duties. Users must request, in writing, permission to use webmail or Citrix from their respective department head, ITD Network Manager and/or IT Director.

## **10. Bring Your Own Device (BYOD)**

With permission from their respective department head, employees may elect to use personally-owned smart phones and/or tablets in support of their job responsibilities. Use of personal devices to access Town ITRs is governed by the Town's supplemental **Bring Your Own Device Policy**.

## **11. No Expectation of Privacy**

Town ITRs are the property of the Town of Wellesley and are to be used in conformance with this policy. The Town retains control over the efficient and proper operation of the workplace, reserves the right to monitor, access, review, copy, store, or delete any electronic communications without prior notice, including personal messages, from any system for any purpose and to disclose them to others, as it deems appropriate. Users should be aware that ITD, in order to ensure proper network operations, routinely monitors network traffic. Use of Town ITRs constitutes express consent for the Town to monitor and/or inspect any data that users create or receive, any messages they send or receive, and any web sites that they access.