Town of Wellesley

Information Technology Resources Policy

Rev. 3.0
November 1, 2016

1. Objective

The Town's objectives in developing this policy are to address the ethical and appropriate use of technology resources, to maintain the security of the network, and to enable Town employees to deliver better services to residents at lower costs. This document formalizes the policy for all Town of Wellesley (Town) employees on the use of **information technology resources**; (ITRs), including computers, printers and other peripherals, programs, data, e-mail, and the Internet.

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. Failure to observe this policy may subject individuals to disciplinary action, including termination of employment. 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).

For purposes of the ITR Policy, "employees" includes all municipal employees as defined in M.G.L. c.268A, §1.

2. Purpose

This Policy is intended to provide guidance on the acceptable use and prohibited uses of the Town of Wellesley's ITRs. It does not intend to identify all authorized or prohibited activities by users; all existing state, federal and local laws and Town policies apply.

3. Acceptable Uses

Employees are encouraged to use ITRs to the fullest extent in pursuit of the Town's goals and objectives. While ITRs are provided for Town business only, 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.

4. Unacceptable Uses

It is unacceptable for any person to use Town ITRs:

- to perpetrate an illegal act, including violation of any criminal or civil laws or regulations, whether state or federal
- for political purpose
- for commercial purpose
- to send threatening or harassing messages, whether sexual or otherwise
- to access or share sexually explicit, obscene, or otherwise inappropriate materials to infringe any intellectual property rights
- to gain, or attempt to gain, unauthorized access to any computer or network
- for any use that causes interference with or disruption of Town ITRs, including propagation of computer viruses or other harmful programs
- to intercept communications intended for other persons
- to misrepresent either the Town or a person's role at the Town

- to distribute chain letters
- to libel or otherwise defame any person
- to access online gambling sites

Unless such use is reasonably related to an employee's job, and permission has been granted by the IT Director or Network Manager, it is unacceptable for any person to use Town ITRs:

- to access social media sites
- to access external email/webmail services
- to access external networks or Internet-based file sharing services

5. Data Confidentiality

In the course of performing their jobs, 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. Additional direction on an employee's responsibility to safeguard personal information is detailed in the Town's *Written Information Security Policy*.

6. 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, employees must respect the rights of intellectual property owners, and exercise care and judgment when copying or distributing computer programs or information that could reasonably be expected to be copyrighted.

7. User Accounts

Employees may be issued a user account for secure access to the network and enterprise applications. An appropriate level of access will be determined by ITD, in consultation with the user's senior management. All network user accounts require strong passwords, to be created by the user according to rules promulgated by ITD, and changed at least once every six months. Users must not share their passwords with anyone else, must keep their passwords in a secure location, and should promptly notify ITD personnel if they suspect their passwords have been compromised. In addition, users who will be leave their PCs unattended for must either log off the network, lock their computer with a password-protected screen saver, or otherwise secure physical access to the computer.

8. Computer Viruses / Malware

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, antivirus software, etc.), but employees should still exercise reasonable precautions in order to prevent the introduction of computer viruses or other malware. Users who are identified as being a source of unauthorized intrusion may be disconnected from the network. Re-establishing connection will be at the discretion of ITD in consultation with the user's senior management.

9. E-mail

Unless not required by job function, all employees will be provided with an @wellesleyma.gov email address. 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. Employees should be aware that all e-mail sent/received through an @wellesleyma.gov account is permanently archived by ITD. Private email (i.e. a commercial email system or service, separate and apart from the Town's primary email system) is not an authorized or official method of communicating business related information.

10. 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. Employees 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.

11. Bring Your Own Device (BYOD)

ITD permits employees to access Town ITRs on personally owned smart phones, tablets, and/or PCs through its "Bring Your Own Device" (BYOD) program. The program is designed to offer employees a choice of personal preference and better integration of their work and personal lives. It is a cost-effective way for the Town to enable employees the flexibility to work in a way that optimizes their productivity. Current use cases for personal device use include email and calendars, virtual desktop (e.g. Citrix), cloud document access, and web-enabled applications.

Use of a personal device is not mandatory, and employees will not be reimbursed (financially, or otherwise) for the business use of a personal voice/data service plan. The Town of Wellesley is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of a personal device for business purposes.

While accessing Town ITRs from personal devices, employees:

- will not download or transfer sensitive business data. Sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a charge/complaint/case, proprietary information, or Town financial operations
- will delete any sensitive business data that may be inadvertently downloaded and stored on the personal device through the normal process of viewing e-mail attachments
- will protect their device with a (minimum) four-digit passcode, and will set their device to lock automatically after a maximum of 5 minutes of inactivity
- will maintain the original personal device operating system and keep it current with security patches and updates, as released by the manufacturer
- will not "jail break" the personal device (installing software that allows the user to bypass standard built-in security features and controls)
- agree to not share the personal device and network accounts with other individuals or family members
- will not connect the personal device to the employee's work PC via (direct or wirelessly) for file transfer or backup purposes, without express permission of the IT Director or Network Manager
- will immediately notify ITD if the personal device is lost or stolen, at which point ITD will change the employee's network password and (in extreme cases) retains the authority to remotely wipe the device

Due to the variety of mobile device types and configurations, ITD is only able to provide limited support for connecting a personal device to Town ITRs, and for use of device software/applications. ITD personnel respect the privacy of your personal device and will only request access to the device to assist with implementation of security controls, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings.

12. Acknowledgement

ITD shall review this policy at least annually, and may propose changes to the Board of Selectmen at any time. Notice of any changes will be provided to all employees.

By signing below, the employee acknowledges that he/she understands and will comply with the Town of Wellesley Information Technology Resources Policy.

Employee Name: _____

Employee Signature: _____ Date: _____

Promulgated this 1st day of November, 2016, effective upon the filing of a copy hereof with the Town Clerk.

WELLESLEY BOARD OF SELECTMEN

Marjorie R. Freiman, Chair

Ellen F. Gibbs, Vice Chair

David L. Murphy, Secretary

Barbara D. Searle

Jack Morgan

Town of Wellesley

Written Information Security Policy

Rev. 1.0
November 1, 2016

1. Objective

The Town's objective in developing and implementing this comprehensive written information security policy ("WISP") is to create effective administrative, technical and physical safeguards for the protection of personal information of residents of the Commonwealth of Massachusetts. This WISP sets forth our procedures for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information.

For purposes of the WISP, **"personal information"** is defined as: "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."

For purposes of the WISP, "employees" includes all municipal employees as defined in M.G.L. c.268A, §1.

2. Purpose

The purposes of the WISP are to ensure the security and confidentiality of personal information; protect against anticipated threats or hazards to the security or integrity of such information; and to protect against unauthorized access to or use of such information that creates a substantial risk of identity theft or fraud.

3. Scope

In formulating and implementing the Policy, the Town has addressed and incorporated the following protocols:

- Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;
- Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
- Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
- Designed and implemented a WISP that puts safeguards in place to minimize those risks; and,
- Implemented regular monitoring of the effectiveness of those safeguards.

4. Data Security Compliance Officer

The Town has designated the Information Technology Director to implement, supervise and maintain the WISP. This designated employee (the "Data Security Compliance Officer") will be responsible for the following:

- Initial implementation of the WISP;
- Providing ongoing training as appropriate for all Town employees, including temporary and contract employees, who have access to personal information, on the elements of the WISP;
- Regular testing of the WISP's safeguards;

- Evaluating the ability of third-party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access; and requiring such third party service providers by contract to implement and maintain appropriate security measures;
- Reviewing the security measures in the WISP at least annually, or whenever there is a material change in our business practices or applicable federal and state regulations that may implicate the security or integrity of records containing personal information;
- Consulting and apprising the Executive Director and Board of Selectmen of all reviews, including any recommendations for improved security arising from the review.

5. Internal Risk Mitigation Policies

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

- We will only collect personal information that is necessary to accomplish our legitimate transactions or to comply with any and all federal, state or local regulations.
- Access to records containing personal information shall be limited to those employees who have a legitimate need to access said records, and only for this legitimate purpose.
- A copy of the WISP is to be distributed to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility for acknowledging in writing, by signing the attached sheet, that he/she has received a copy of the WISP and will abide by its provisions.
- Each department shall develop rules to ensure that reasonable restrictions for physical access to records containing personal information are in place; and each department must store such records and data in locked facilities, secure storage areas, or locked containers.
- A terminated employee's physical and electronic access to records containing personal information shall be restricted at the time of termination. This shall include remote electronic access to personal records, voicemail, internet, and email access. All keys, keycards, access devices and the like shall be surrendered at the time of termination.
- Terminated employees must return all records containing personal data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any device owned directly by the terminated employee.
- Access to electronically stored personal information is restricted to approved and active user accounts.
- Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall be disposed of only in a manner that complies with M.G.L. c.93I.
- Employees are required to report suspicious or unauthorized use of personal information to a supervisor or the Data Security Compliance Officer.
- Whenever there is an incident that requires notification pursuant M.G.L. c.93H, the Data Security Compliance Officer shall host a mandatory post-incident review of events and actions taken, if any, in order to determine how to alter security practices to better safeguard personal information.
- Disciplinary action will be applicable to violations of the WISP, irrespective of whether personal data was actually accessed or used without authorization.

6. External Risk Mitigation Policies

To guard against external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and shall be implemented immediately:

- Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes personal information.
- All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any computer that stores or processes personal information.
- Personal information shall not be removed from Town facilities in electronic or written form absent legitimate need and use of reasonable security measures, as described in this policy.

- To the extent technically feasible, all personal information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible. Encryption means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by law.
- The Town's *Information Technology Resources Policy* shall contain secure user authentication protocols that:
    - Control user ID and other identifiers;
    - Assign passwords in a manner that conforms to accepted security standards;
    - Control passwords to ensure that password information is secure.

7. Breach of Data Security Protocol

Should any employee know of a security breach at any of our facilities, or that any unencrypted personal information has been lost or stolen or accessed without authorization, or that encrypted personal information along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the following protocol is to be followed:

- Employees are to notify the Data Security Compliance Officer in the event of a known or suspected security breach or unauthorized use of personal information.
- The Data Security Compliance Officer shall be responsible for drafting a security breach notification to be provided to the Massachusetts Office of Consumer Affairs and Business Regulation and the Massachusetts Attorney General's office. The security breach notification shall include the following:
    - A detailed description of the nature and circumstances of the security breach or unauthorized acquisition or use of personal information;
    - The number of Massachusetts residents affected at the time the notification is submitted;
    - The steps already taken relative to the incident;
    - Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and
    - Information regarding whether law enforcement officials are engaged in investigating the incident.

8. Acknowledgement

The Data Security Compliance Officer shall review this Policy at least annually, and may propose changes to the Board of Selectmen at any time. Notice of any changes will be provided to all employees.

By signing below, the employee acknowledges that he/she understands and will comply with the Town of Wellesley Written Information Security Policy.

Employee Name: _____

Employee Signature: _____ Date: _____

Promulgated this 1st day of November, 2016, effective upon the filing of a copy hereof with the Town Clerk.

WELLESLEY BOARD OF SELECTMEN

Marjorie R. Freiman, Chair

Ellen F. Gibbs, Vice Chair

David L. Murphy, Secretary

Barbara D. Searle

Jack Morgan