TOWN OF HOLLISTON
TECHNOLOGY PROCEDURES

Employee Technology Acceptable Use Policy

Purpose

To establish a Town of Holliston Employee Acceptable Use Policy and Procedure for all Town employees (union and non-collective bargaining employees excluding School Department Employees which fall under a different Acceptable Use Policy).

Policy

The Acceptable Use Policy (AUP) is intended to outline expected behavior in regards to the use of Holliston Information Technology (IT) resources and to delineate between authorized and unauthorized operating procedures. The AUP also provides an overview of IT system security policies mandated by the Town of Holliston. All Town IT resources, including but not limited to, hardware, software, storage media, and computer, email, and network accounts, provided by the Town of Holliston are the property of the Town. They are to be used for business purposes in serving the interests of the Town and Town residents in the course of normal operations. Use of Holliston resources for the purposes other than those identified within this policy or in accordance of your job description are strictly prohibited and could negate the security of Holliston's IT Systems and be cause for termination. Effective IT security is a team effort involving the participation and support of everyone who deals with information and/or information systems. It is the responsibility of everyone to know these guidelines, and to conduct their activities accordingly.

Procedures

1. The Town of Holliston realizes an Employee may at times (during breaks, lunches, and down-time) use Holliston IT resources for non-work purposes but the following activities are not allowed both for work and non-work related activities:

a. create, copy, transmit, or retransmit greeting cards, video, sound or other large file attachments that can degrade the performance of the entire network or expose the network to unwanted malware and viruses;

b. access inappropriate websites or known hacker sites;

c. use Holliston IT systems as a staging ground or platform to gain access to other computer systems.

d. use Holliston IT resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities, include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation;

e. create, download, view, store, copy, or transmit explicit or obscene materials;

f. create, download, view, store, copy, or transmit materials related to any gambling (legal or illegal), illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited;

g. download, copy, and/or play of online computer video games;

h. use Holliston IT resources for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity including assisting relatives, friends, or other persons in such activities

i. post confidential Town of Holliston information to external news groups, bulletin boards, social media (e.g. Facebook, Twitter) or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Town employee, unless appropriate Department approval has been obtained or the use is not at odds with the Department's Mission.

j. acquire, use, reproduce, transmit, or distribute any controlled information, including computer software and data, that includes privacy information, copyrighted, trademarked, or material with other intellectual property rights (beyond fair use).

k. download files, for example music or other inappropriate material, for the purpose of forwarding them to another individual. This activity, also known as "file sharing" creates a substantial computer security risk in that it may facilitate the spread of computer viruses.

2. All employees must remain alert to malicious software often transmitted via email and website browsing. Installing and/or executing any foreign files or software on an individual computer may result in damage to your computer or compromise the security of sensitive Town records. It is therefore imperative the employees exercise appropriate caution in their electronic communications and report any suspicious email or file to the Town of Holliston Technology Department for review.

3. Town of Holliston E-mail Accounts

a. Employees will be issued a Town of Holliston Email Account upon employment.

b. Employees are responsible for maintaining the security of their Holliston email account and to take precautions to prevent unauthorized access to their email.

c. Employees must not open any files attached to an unsolicited or unexpected email. Unsolicited email is defined as any email message received that was mailed from an unknown,

suspicious, or untrustworthy source or via mass mailing list to which you are not subscribed to. These messages can include inappropriate topics, hoax messages, chain emails, spam messages, and other advertisement messages.

d. Employees must not create, transmit, or forward chain letters (a message directing the recipient to forward it to multiple people, typically promising rewards for compliance) or other unauthorized mass mailings regardless of subject matter.

e. Employees must delete spam and other junk emails without forwarding it.

f. When an unsolicited email is received users must not select an option to "opt out" of future mailings as this is often a method by the sender to confirm a valid email address and usually results in more spam.

g. Employees must not click on or follow any hyperlinks or URL's included in an unsolicited email message.

Email Privacy. Email is a Town of Holliston asset and a critical component of the communication system. An email account is provided by the Town of Holliston for users to facilitate the performance of their work and all correspondences are the property of the Town of Holliston. Holliston's Town Administrator and Technology Staff reserves the right to retrieve and view the contents for legitimate reasons, such as to find lost messages, to comply with investigations or legal requests, to recover from system failures, or to fulfill FOIA requests. The Town of Holliston also reserves the right to implement security policies to detect, block, or quarantine inappropriate or threatening emails (both incoming and outgoing) and attachments. As necessary, incoming and outgoing email may be retrieved as part of this policy. Holliston Employees should be aware that a copy of every message drafted and/or sent through the Holliston Email Account, even if deleted immediately, is archived and could be retrieved to meet legal and FOIA requirements.

4. Personal Email Account Usage

a. Employees with Holliston Email accounts and access to Holliston technology equipment must not use non-Holliston Email accounts (e.g. personal Gmail accounts, Hotmail, Yahoo, AOL) for conducting official employment duties. The Holliston Email system has safeguards in place to allow for archiving, recovering, and security checks.

b. Employees are allowed to access their personal email on Town equipment provided you access the email through a website (e.g mail.google.com or www.hotmail.com.) Personal email client software (Outlook, AOL Desktop, Google Desktop) must NOT be installed on Town equipment to view personal email.

c. Do not open any links from personal emails or open any attachments from personal emails. This is the number one way viruses are brought into the Town's computer system.

5. Desktop/Laptop/Tablet Usage

a. All laptop, desktop, and tablet computers and installed software are assigned to users on an individual (or department) basis. Employees must take every reasonable precaution to protect such resources from loss or damage.

b. Employees must not change any security settings on their workstation. If changes are required please inform the Technology Department who will make the appropriate changes.

c. Employees must not leave their workstation unattended and unprotected. Press Ctrl-Alt-Delete and select "Lock this Computer" if you are leaving it unattended.

d. Employees must not install personal equipment or software on a Town of Holliston computer without prior approval from the Technology Department

6. Privacy Expectations: Employees do not have a right, nor should they have any reasonable expectation, or privacy while using any Holliston IT resources at any time, including accessing the Internet or using email. By using Holliston IT resources, employees give their consent to disclosing the contents of any files or information maintained using this equipment. In addition to access by Holliston Officials, data maintained on Holliston IT resources may be subject to discovery and Freedom of Information Requests. By using Holliston Office equipment, consent to monitoring is implied including accessing the Internet or using email.