Information Technology Resources Acceptable Use Policy

The City's Information Technology Resources Acceptable Use Policy concerns the acceptable uses of information technology resources provided by the City. This policy concerns, among other matters, the use of computers, electronic mail ("email"), and the Internet connection generally. This policy applies to the access and use of the City's information technology resources by any employee, independent contractor, student, intern, extern, volunteer, guest, or any other person who accesses or uses the City's information technology resources.

1. Definitions

"Information technology resources" refers to all of the City's information technology systems and accessories, including, but not limited to: local and wide area networks; the City-wide area network; the Internet; computers, workstations, and laptops; printers; fax machines; servers; access to research databases and services; City-owned cellular phones, smartphones, and other personal digital assistants (PDAs); software programs; email; data; and any other communications equipment or peripheral equipment. "User" refers to City employees, independent contractors, students, interns, externs, volunteers, guests, and all other individuals who access or use the City's information technology resources.

2. Responsibilities of All Users

Use of information technology resources is conditioned upon and subject to the City's Information Technology Resources Acceptable Use Policy. In addition to the policy contained herein, usage must be in accordance with all other applicable City policies and all applicable Commonwealth and federal laws. Users shall exercise reasonable care and precautions in using, transporting, securing, and otherwise handling City-owned information technology resources, including both hardware and software. Laptop computers ("laptops") may be easily damaged and stolen. A user traveling with a laptop shall take reasonable care and precautions to prevent damage and theft of the laptop. Users must immediately report any damage or theft of information technology resources to their supervisor or Department Head. Users must also exercise reasonable care and precautions to prevent the introduction of a computer virus into any of the City's networks.

All network communications, including Internet communications, identify the user to all sites accessed. City email addresses assigned to employees and other authorized users identify the sender as a member of the City. Internet access and email, like all other forms of communication, reflect upon the City. Thus, users should maintain a professional and courteous tone, observing the rules and policies governing conduct of employees. A user should not use a City email account for personal, non-City purposes, including, but not limited to, using City email for social media websites such as Facebook and Twitter, unless properly authorized to do so. Signing up for newsletters and other emails that are not related to City work is also prohibited.

3. Software Piracy and Copyright Infringement

The City is committed to providing its employees and other users with the tools to do their work, including, if applicable, a computer and appropriate software. The City will only do so, however, in compliance with all of its vendors' licenses and applicable copyright laws. Computer programs are legally protected intellectual property, and software publishers license their programs to

protect their property rights from infringement. Under no circumstances may employees or other users unlawfully copy or distribute any software or copyrighted information. The use of software from unauthorized sources may also present security threats or interfere with the proper functioning of the City's networks. No unauthorized software or other executable programs shall be installed or used on any component of the City's information technology resources, particularly computers, workstations, and City-owned cellular phones and smartphones.

4. **Monitoring and No Expectation of Privacy**

City information technology resources, including Internet access and email, are the property of the City. As such, the City retains the right to inspect any user's computer and the files contained therein. The firewall between the Internet and the network automatically checks all data moving between the network and the Internet, identifying the sending and receiving destinations. Individual computer and workstation activity is logged and monitored, and any files created or received by users, any messages sent or received by users, and any Internet websites accessed by users are subject to monitoring at all times. In addition, any and all use of the City's information technology resources is subject to monitoring by the City at any time without notice and notwithstanding any password(s).

Therefore, users should have no expectation of privacy in any access or use of the City's information technology resources, including, but not limited to, data, incoming and outgoing emails and attachments, Internet websites accessed or viewed, and files downloaded. In fact, the mere deletion of emails, data, or files may not eliminate them from the system.

Use of the City's information technology resources constitutes consent to monitoring and is conditioned upon strict adherence to the City's Information Technology Resources Acceptable Use Policy.

5. Personal Software and Hardware

No personally owned software, peripheral device, or other accessory shall be used in, or attached to, any equipment or device that is part of the City's information technology resources. Flash drives may be used if approved in advance by a supervisor or Department Head. The flash drive should be empty when first used and must be used only for City- or work-related documents and other approved purposes.

6. Prohibited Conduct

No user shall access, use, or otherwise utilize any of the City's information technology resources: (1) in furtherance of any illegal act, including violation of any Commonwealth or federal laws or regulations; (2) for any political purpose or to make solicitations in violation of the Commonwealth's Campaign Finance Law, G. L. c. 55; (3) for any commercial purpose or solicitation, including, but not limited to, the offering, providing, leasing, or purchasing of products or services;
(4) to access online gambling websites, or for any gambling or related activity whether or not such activity violates Commonwealth or federal law;
(5) to violate any copyright laws or to infringe upon any intellectual property rights;
(6) For visiting Internet websites with inappropriate adult content or pornography;

(7) to send or display threatening or harassing images, emails, messages, or materials, including, but not limited to: messages, materials, or images of a sexual nature; racial, ethnic, sexual, religious, or gender-based slurs; or messages or images that offensively address someone's age, ancestry, color, creed, disability, ethnicity, family status, gender, genetic information, marital status, military status, national origin, political affiliation, pregnancy, race, religion, sex, sexual orientation, or veteran status, including comments posted on, or messages sent via, blogs, social media websites (e.g., Facebook, Twitter), or any other websites;
(8) To libel or otherwise defame any person, group, business, or other entity;
(9) To access, display, or share sexually explicit, obscene, or otherwise inappropriate materials, messages, or images;
(10) To distribute chain letters or other similar communications;
(11) To distribute confidential City information that would violate City policy or Commonwealth or federal law;
(12) To intercept, or attempt to intercept, a communication intended for another person;
(13) To gain, or attempt to gain, unauthorized access to any computer or network;
(14) for any use that causes interference with, or disruption of, network users and/or any of the City's information technology resources, including propagation of computer viruses or other harmful programs;
(15) To misrepresent either the City or a person's role with the City;
(16) To download and/or install non-City supported and licensed software applications or programs;
(17) To connect unauthorized or unapproved computers, printers, or other peripherals or devices to any of the City's networks;
(18) To develop or use programs that harass other users or infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system, or network;
(19) To establish unauthorized connections that create routing patterns that are inconsistent with the effective and shared use of any of the City's networks;
(20) To modify or access any City records, unless such records are within the user's scope of authorized access and responsibility;
(21) To access, display, or disseminate material that advocates violence or discrimination toward other people (Le., hate literature); or
(22) In any manner that is prohibited by this policy or any other policy of the City, or in any unprofessional manner.

The foregoing list is not intended to be an exhaustive list of prohibited conduct. All questions regarding what may constitute an acceptable use or prohibited conduct under the City's Information Technology Resources Acceptable Use Policy should be addressed to the City Solicitor.

7. **Email**
Word processing software documents, portable document format ("PDF") files, and other similarly formatted files related to the user's work for the City are allowed to be sent, received, and downloaded as attachments.

No personal pictures, screensavers, executable programs, videos, or other potentially malicious files shall be downloaded. Video and audio unrelated to a user's work for the City shall not be streamed over the Internet while using a networked computer. These types of streaming can slow down the network and prohibit users from being able to complete work-related tasks. The City strives to protect the security of its networks. Therefore, if a user has any doubt about the source, nature, or potential hazard of a file or attachment, the user shall not download the file or attachment from the Internet or via email.

A user shall only access his City email account from the user's home or other non-City-owned location upon the express prior permission of his Department Head or applicable supervising authority.

No user may send a citywide email or other broadcast for any reason unrelated to the user's work for the City without the express prior permission of the City Solicitor.

8. **Public Records**

Emails and other messages created or received by a user utilizing the City's information technology resources, including any associated attachments, may constitute a public record under G. L. c. 4, § 7(26) and therefore may be subject to public disclosure under the Commonwealth's Public Records Law, G. L. c. 66. Additionally, emails and other messages may be discoverable in litigation and may be admissible in court. Therefore, users should not expect that emails or other messages, including those marked "personal" and/or "confidential," are private or confidential.

Users shall not read email and other messages that are received by another employee when there is no work-related purpose for doing so. Users shall not send emails or other messages, or access the Internet under another user's name or password without prior authorization. A user shall not change any portion of a previously sent email or other message without prior authorization from the author of the previously sent email or other message; however, a user may delete, in its entirety, a previously sent email or other message that is part of a subsequent email or other message (e.g., a forwarded email).

The records of emails and other messages created or received by a user utilizing the City's information technology resources, including any associated attachments, are subject to the same rules regarding record retention and disposition as are paper records.

9. **Conflicts of Interest and Political Activities**

An employee's or other user's use of the City's information technology resources must not conflict with the Commonwealth's Conflict of Interest Law, G.L.C. 268A, or the Commonwealth's Campaign Finance Law, G. L. c. 55. All questions regarding conflicts of interest and political activities should be addressed to the City Solicitor.

10. **Data Confidentiality**

In the course of providing services to the public, to City departments, and to other *government* agencies, users often *have* access to confidential information, such as personal data about identifiable individuals. Under no circumstances is it permissible for any user to access, or to acquire access to, confidential data, unless such access is required by the user's job. Under no

circumstances may users disseminate any confidential information, unless such dissemination is required by their jobs, or if prior permission has been granted by the owner(s) of the confidential information.

11. Security
Users must take particular care to *avoid* compromising the security of all City networks. All passwords must be kept confidential. Users who will be leaving their personal computers, workstations, or other hardware unattended for extended periods of time should log off or lock their *device* so as to prevent unauthorized access to the *device* and/or to any City network.

All messages of any kind, including, but not limited to, emails created, sent, or retrieved *via* the Internet or any City network, are the property of the City and should be considered public information. The City reserves the right to access and to monitor all messages and files on any City network or system as deemed necessary and appropriate, including, but not limited to, blocking website software.

12**. Consequences** of Violation of Policy
Use of the City's information technology resources is a privilege that may be revoked at any time by the City, including, but not limited to, for any conduct that violates the City's Information Technology Resources Acceptable Use Policy. Any employee or other user who violates the City's Information Technology Resources Acceptable Use Policy shall be subject to disciplinary action, up to and including termination. In appropriate circumstances, the City may refer the matter to law enforcement officials for possible prosecution.

13. **Receipt and Acknowledgment**
The Personnel Administrator shall provide annually to all employees and other users, and to new employees and other users upon their employment or other association with the City, an individual written copy of the City's Information Technology Resources Acceptable Use Policy. The Personnel Administrator shall also provide all employees and other users with an individual written copy of an updated Information Technology Resources Acceptable Use Policy. Every employee and other user must read the City's Information Technology Resources Acceptable Use Policy, familiarize himself with the material therein, and sign the Acknowledgement Form distributed by the Personnel Administrator.

All employees and other users must submit to the Personnel Department, within thirty (30) days of their date of hire and within thirty (30) days of the date of receipt of an updated Information Technology Resources Acceptable Use Policy, a signed Acknowledgment Form certifying that they have received a copy of the City's Technology Resources Acceptable Use Policy and that they understand that they are required to abide by the City's Technology Resources Acceptable Use Policy.

No employee or other user shall receive authorized access to any of the City's information technology resources until the employee or other user has submitted a signed Acknowledgment Form to the Personnel Administrator.