DEPARTMENT OF PERSONNEL, CITY HALL, 70 ALLEN STREET, ROOM 107, PITTSFIELD, MA 01201 PHONE: 413-499-9340

INTERNET & COMPUTER POLICY

Introduction

The City of Pittsfield (hereinafter, the "City") provides employees access to the vast information resources of the Internet with the intention of increasing productivity. While the Internet has the potential to help employees do their job faster or smarter, there is justifiable concern that it can also be misused. Such misuse can waste time and potentially violate laws, ordinances, or other City policies. This Internet usage policy is designed to help employees understand the expectations for the use of these resources.

The underlying philosophy of this policy is that Internet access from the City is for business related purposes, including communicating with colleagues, researching relevant topics and obtaining useful information. In addition, all existing laws and City policies apply to your conduct on the Internet, especially those that deal with intellectual property protection, privacy, misuse of City resources, sexual harassment, data security, and confidentiality.

This policy sets forth general guidelines and examples of prohibited uses of the Internet for illustrative purposes, but does not attempt to state all required or prohibited activities by employees. Employees who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the Information Technology Department. Moreover, these rules may be supplemented by more specific administrative procedures and rules governing day-to-day management and operation of the City's computer system. Collaboratively, this policy will be monitored and administered by the Information Technology Department and Personnel Department.

Internet Guidelines

A. Use for Official City Business: It is the City's policy to limit Internet access to official City business.

B. Authorization: Authorization for Internet access must be obtained through the Information Technology Department. Once authorization is approved, each employee is responsible for the security of his or her account password and will be held responsible for all use or misuse of their account. Each employee must maintain secure passwords and never use an account assigned to another user, unless specifically authorized to do so.

C. Compliance: The City Internet facilities and computing resources must not be used to knowingly violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, or local jurisdiction in any material way. United States copyright and patent laws protect the interests of authors and software developers in their products. It is against federal law and City policy to violate the copyrights or patents of others on or through the Internet.

D. Viruses: No employee may use the City's Internet facilities 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. Computer files, including attachments that are downloaded and/or opened from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions should be taken to detect viruses and to prevent the infection of other computers. Employees shall direct any questions pertaining to the proper use of virus detection software to the Information Technology Department prior to the downloading and/or opening of any computer files, including attachments.

E. Employee Integrity: Each City employee using the City's Internet shall identify themselves honestly, accurately, and completely when corresponding or participating in interactive activities.

F. Information Acquired from the Internet: The City has no control or responsibility for content on an external server not under the control of the City. The truth or accuracy of information on the Internet and in e-mail should be considered suspect until confirmed by a separate and reliable source.

G. City monitoring: Employees should not have any expectation of privacy as to his or her computer or Internet usage, including the receipt and sending of e-mail. It is possible for the City to monitor Internet usage patterns, and the City may inspect, without limitation, any computer system used by an employee, including files stored either on the computer hard drive or the City's server to the extent necessary to ensure compliance with this Policy.

H. Alternate Connections: Alternate Internet Service Provider connections to the City's internal network are not permitted unless expressly authorized and properly protected by an appropriate security device.

I. Use of Computers: All computer hardware shall at all times remain the property of the City of Pittsfield, until otherwise disposed, and may not be removed from their respective sites without the express written approval of the Information Technology Department. The installation or upgrade of computer software programs on computer hardware, without the express written approval of the Information Technology Department, is strictly prohibited. The City may issue more specific administrative procedures and rules governing employee use of computer hardware.

J. Prohibited Practices:

(1) Employees shall not use City computers knowingly to 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 purposes is strictly prohibited.

(2) Employees shall not make an unauthorized attempt to enter into another employee's computer (commonly referred to as "hacking"). Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.

(3) Employees shall not connect personal cell phones or any personal electronic device to a city owned computer for any reason.

(4) Employees shall not disclose confidential information or promote personal political beliefs, discrimination, sexual harassment, and any unlawful activity; nor shall the City's computers be used by employees for private financial gain, or commercial, advertising or solicitation purposes.

(5) Employees shall not use City computers to display any kind of image or document that is obscene, pornographic, sexually explicit or sexually suggestive. Additionally, these materials may not be archived, stored, distributed, edited, or recorded using City network, printing, or computing resources.

(6) Employees shall not use City computers to receive or transmit information relating to union business, which shall include but not be limited to communications pertaining to union meetings, policies, practices, negotiations and disputes and Internet sites dedicated to such topics. Communication between union officials and their counsel is permitted but not between union members.

(7) Employees shall not access non-city sanctioned file sharing Internet sites or internet radio streaming services; nor shall employees use e-mail for the purpose of sending chain-letters and unsolicited mass electronic mail, or cause the receipt of unsolicited mass electronic mail.

(8) Employees shall not use their City of Pittsfield assigned email address to sign up for newsletters, mailing lists, newsgroups, etc., unless these are work related. Employees shall not use their City of Pittsfield assigned email address to sign up for marketing materials through shopping sites. The City of Pittsfield assigned email address is to be used for work only and not for any type of personal correspondence, shopping, etc.

(9) Employees shall not maliciously use or disrupt the City's computers, networks, Internet services; nor breach the system's security features; nor misuse or damage the City's computer equipment; nor misuse computer passwords or accounts; nor attempt to access unauthorized sites; nor use the City's computers,

networks and Internet services after such access has been denied or revoked; nor attempt to delete, erase or otherwise conceal any information stored on a City computer that violates this Policy.

(10) Social Media Sites. Social media sites and services, including but not limited to Facebook and Twitter, shall not be accessed from City-owned equipment unless the access is for official City business and is approved by the employee's department head or appointing authority for a public purpose. Employees are cautioned that inappropriate postings to social media sites on personal time and/or using personal devices and accounts may subject the employee to discipline, up to and including termination, if the postings adversely affect the City or the employee's workplace. By way of example, and not by way of limitation, inappropriate personal postings that may subject an employee to discipline include but is not limited to threats of violence, bullying, comments suggesting that the employee harbors any animosity or bias towards any protected class of individuals or any individual member of a protected class, and the disclosure of personal information or other confidential information collected in the workplace. More information may be found in the City's Workplace Violence Policy. Additionally, please refer to the City's Social Media Creation and Content Policy for entire protocols and procedures regarding Social Media websites and accounts.

K. Electronic Mail:

(1) The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third party. Employees must exercise caution and care when transferring such material in any form. Each and every electronic communication sent by an employee must include the following message:

"This electronic message is confidential and intended for the named recipient only. Any dissemination, disclosure or distribution of the contents of this communication is unlawful and prohibited. If you have received this message in error, please contact by return e-mail or telephone 413-(Department's Telephone Number), and delete the copy you received. Thank you."

(2) It has been determined by the Secretary of State's Office of the Commonwealth that electronic mail qualifies as "public records", as same are defined in Chapter 4, section 7(26) of the Massachusetts General Laws. All electronic mail sent or received by employees through the Internet shall be archived by the Information Technology Department. All employees shall retain either a printed or digital record of electronic mail sent or received over the Internet, in the same manner as other records are kept by their Departments.

Violation of Policy

A violation of this Policy will result in either the suspension or permanent loss of the privilege to use the Internet and the City's computers. It will also result in disciplinary action being taken against the employee, up to and including termination from employment. Additionally, employees shall be personally liable for any losses, costs or damages incurred by the City related to violations of this Policy. The illegal use of the City's computers will result in referral to law enforcement authorities. Employees shall report violations of this Policy to their supervisor, or in the case of department heads, directly to the Personnel Director. Retaliation against another employee 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 City. Please refer to the City's Workplace Violence Policy regarding harassment and retaliation.