City of Saint Paul
Internet Access and Email Policy
May 11, 2015

Internet and Email Policy
The city provides Internet access and electronic mail (email) capabilities to employees at city expense to further city business. Anyone using the city's Internet access and electronic mail must comply with this Internet Access and Email Policy ("Policy").

The purpose of this Policy is to require the proper use, and to prohibit improper use of these public resources. This Policy is a minimum standard for use of email and Internet access, and department and office directors have the authority to apply additional or more restrictive standards to govern specific situations affecting their operations. The city does not intend to create contractual rights by this Policy, and reserves the right to unilaterally change it at any time.

Privacy
The city and its officials reserve the right to monitor and/or log all network, Internet activity and email use and content accessed via city equipment or systems; and to access, review, read, disclose and use all records and all content in any way it deems necessary. This monitoring may include, but is not limited to, accessing computers, hard drives, attached/connected devices, external media, flash drives, disks and adjacent work areas. No person should expect that any message or its contents, or any record of use, whether for city business, personal use or a prohibited use, will be private, even where a personal password in used.

Personal Use of Email and Internet Access
Incidental and occasional personal use of email and Internet access is tolerated subject to the same policies, procedures and legal considerations that apply to business-related email and Internet use. Incidental and occasional personal use must be done on employee time such as during lunch or breaks. Such personal use is permissible so long as the incremental cost is negligible, no city business activity is preempted by the personal use, and no city policies or laws are violated. Excessive personal use and personal use in violation of this policy can be grounds for discipline up to and including termination. Personal use of the city's Internet access and email constitutes the user's consent to the city to monitor, read, and use in any way any message, record, or other information created by the personal use.

Use of a personal email account accessed via city department equipment is allowed under the conditions as set forth above and subject to all of the conditions as set forth in this policy.

Applicability to All Users
This Policy applies to all city Internet and email users including, but not limited to, city employees, whether full-time, part-time, temporary, provisional or otherwise designated. It also applies to all contractors, consultants, volunteers, agents or any other persons who have gained or are given access to the city's Internet service and/or email system.

Acceptable Uses of Internet Access and Email
The following are examples of the acceptable use of the Internet and email:

- Communicating and exchanging information directly related to the mission or work tasks of the city department or office;
- Searching the Internet for information relating to current projects or responsibilities required by official job duties;
- Searching for and using information for purposes of job-related training, professional development, or to maintain currency of education;
- Communicating and exchanging information to enhance existing job-related skills and to participate in professional societies and organizations related to the employee's duties and responsibilities;
- Use of social media for the purposes of community building and engagement provided the employee has permission from their Office or Department Director to use social media on behalf of the city. Employees are prohibited from creating personal social media accounts with city names or logos. (Social media can take many different forms, including but not limited to: Internet forums, weblogs, social blogs, microblogging, wikis, podcasts, pictures, video, rating and social bookmarking.)

Prohibited Uses of Internet Access and Email
Prohibited uses include, but are not limited to:

- Using email or the city's Internet connection to send, view, store, or receive sexually explicit, oriented or related material. Receipt of unsolicited sexually explicit material does not violate this Policy if the user immediately deletes the material and does not further circulate the material. When necessary for legitimate city business, a department or office director may, in writing, authorize a user to access sexually explicit material;
- Using email or the city's Internet connect for commercial purposes, nongovernmental-related fund raising, or for private gain;
- Using email or the city's Internet connection for any form of gambling that violates the city's Gambling Policy;
- Soliciting funds (except for activities authorized pursuant to Chapter 41 of the Administrative Code), exchanging political messages, endorsements, opinions or any other similar persuasive activity;
- Harassing, threatening, defamatory, false, inaccurate, abusive, discriminatory, offensive or other types of messages that violate the city's Workplace Conduct Policy and Procedures, or state or city Human Rights legislation;
- Using email or the city's Internet connection for communication that violates the Minnesota Data Practices Act or any city, state or federal law;
- Defeating or attempting to defeat, through action or inaction, the security system that is set up to protect the city's or other computer systems, unless specifically authorized in writing to do so as part of an employee's official duties;
- Illegal copying, transferring, and/or downloading of pirated and/or copyrighted software or data;
- Installing any authorized equipment;

- Installing and/or using shareware, freeware, public domain software, and software distributed via electronic bulletin boards, the Internet, or other online sources, including radio software available on the city's website, unless authorized in writing to do so by Director of Technology and Communications, or his/her designee;
- Installing or using file sharing programs, especially those programs which circumvent the city's security systems (including downloading and use of file sharing networks on the Internet such as Napster, Morpheous, Gnutella, Aimster, etc.);
- Installing or using instant messaging and chat programs that do not meet the city's security standards;
- Installing or using "backdoor" communications to the Internet such as having a phone line connected to a modem residing within a PC or laptop computer that is also connected to the city's network infrastructure.

Shareware Downloading and Use Exception
When shareware, freeware, public domain software, or non-city online source constitutes the only practical sources of required software, the software is to be thoroughly examined and tested for viruses and approved by the Director of Technology and Communications or his/her designee, before being installed on city computers.

Citywide Messages
The number and length of citywide message sent on the city's network should be kept to a minimum. City directors, or their designee(s), must specifically authorize sending citywide messages through the email system. Many citywide messages, which are used to send the same or similar information to every user, should be posted on the city's Intranet (electronic bulletin board) at http://spnet.stpaul.city/.

Penalty for Noncompliance
City employees and others who are provided access to the city's Internet connection and email services are responsible for knowing and following this Policy. Any person who violates this Policy for the use of Internet access and email may be removed from Internet access and/or the email system and subject to appropriate disciplinary action up to and including termination. Nonemployees, who are allowed access to the city's Internet connection and email service and who violate these standards, may have their contract revoked. All other legal remedies may be pursued.

Responsibility for Compliance
Department and office directors, or their designated representatives, are responsible for enforcing the city's Internet Access and Email Policy. These responsibilities include, but are not limited to:

- Monitoring employee use and reporting suspected noncompliance with the provisions of the city's Policy;
- Revoking service to employees, with or without notice, when deemed necessary for the operation and/or integrity of the city's communications infrastructure and networks;
- Proceeding with appropriate disciplinary action, up to and including discharge, for instances of noncompliance with this Policy;

- Working with Office of Technology – Operations staff to select and install appropriate Internet filtering software.

The Office of Technology and Communications Director, or his/her designated representative, will provide the following services in support of this Policy:

- Maintaining Internet filtering software for all city users;
- Providing assistance to department and office directors to enforce the city's Internet Access and Email Policy;
- Assisting department and office directors, as requested, with electronic tools and training to investigate violations of this Policy.

Effective Date and Consent to Standards
City employees and others who are provided access to city Internet and email access are responsible for knowing and following this Policy. A policy acknowledgement form must be signed by every user of the city's Internet and email system, and kept on file by each department and office director, or their designee, in accordance with appropriate records retention policies.

Questions: Office of Technology and Communications: 651-266-6786