

TECHNOLOGY USE POLICY

Purpose

The purpose of these policies is to assist the City in protecting its computer system security and assets, to protect the privacy rights of employees, to manage City resources, and to protect the rights of third parties for appropriate access to City files

This policy governs access to and appropriate use of City Technology (including but not limited to computers, Internet, E-Mail, cellular phones, desktop phones, and digital equipment). Abuse of the system, including inappropriate content, unauthorized personnel using the system, or unauthorized access to certain equipment and computer files, may result in disciplinary action up to and including discharge.

Policy

The City intends to honor these policies but reserves the right to change them at any time with such prior notices, if any, as the City may deem reasonable under the circumstances.

All employees that work with the City's computers are responsible for reading and adhering to these policies. It is the responsibility of supervisors to ensure that each of their employees have received this document and have signed off that they have read it.

Appropriate Use

The use of City technology such as, but not limited to, computers, Internet and E-Mail systems are City property to be used for City business purposes, and to increase the timeliness and effectiveness of City business communications. While employees may make personal use of City technology during working hours, the amount of use is expected to be limited to incidental use or emergency situations. Excessive time spent on such personal activities during working hours may be subject to disciplinary action.

Incidental and occasional personal use of City technology is allowed to the extent such use:

- (1) Does not interfere with the City's operation of system services or the cost of providing those services.
- (2) Does not interfere with the user's employment or other obligations to the City.
- (3) Is not used for personal monetary gain or for commercial purposes outside of the employee's assigned job duties.
- (4) Does not violate any law, including obscenity, copyright, and defamation laws.

- (5) Does not invade the rights of others.
- (6) Does not violate any other employment policy, including, but not limited to harassment, professionalism, trade secret, and non-disclosure policies.

Department directors and supervisors are responsible for ensuring consistent enforcement of the Appropriate Use Technology policy through training, supervising, and taking disciplinary action if necessary.

Inappropriate Use

Inappropriate uses of City technology include, but are not limited to the following:

- (1) Illegal activities
- (2) Wagering, betting, or selling chances
- (3) Harassment
- (4) Commercial activities
- (5) Activities that result in personal financial gain
- (6) Solicitation, except on City-sanctioned activities/ images
- (7) Pornographic or sexually explicit activities
- (8) Allowing anyone other than City employees access to the Internet or E-Mail
- (9) Activities that demean the dignity of the City
- (10) Engaging in malicious or ill-natured communications
- (11) Other unethical activities

The two exceptions to these rules pertain to the Police Department and the public computers provided by the Public Library. These rules do not apply when a police officer is conducting an authorized criminal investigation. Use of the public computers at the Public Library is subject to rules adopted and enforced by library personnel.

Expectation of Privacy and Transmitting Confidential Information

Employees do not have an expressed or implied personal privacy right in any matter created, received, or sent from City technology.

Security and privacy of messages cannot be guaranteed on Internet and Email systems. Data considered private under the Data Practices Act should not be transmitted in plain text or Email.

Internet Use

The use of the Internet during work hours should be limited to those subjects that are directly related to an individual's job duties for the City of Hibbing. Employees are advised to exercise discretion when using the Internet for personal business since any use can be monitored by individual outside the organization, and **will be** monitored by the City.

The primary function of the computer system is to assist in service delivery to our residents and customers. Allowing employees to spend personal time learning how to use and conduct research on the Internet will ultimately result in improved performance as employees for the City of Hibbing.

To that end, employees may access web sites for personal use after business hours during non-work time. This use is limited to web sites that are considered "business appropriate" and employees are expected to exercise good judgment when accessing sites. Employees may not intentionally access any site that is inappropriate for a public sector employee, or which could cause embarrassment to the organization or the employee. If this occurs, employees are expected to notify their supervisor. Public sector organizations are held to a high standard of scrutiny and ethical behavior. Some examples of inappropriate sites include adult entertainment, sexually explicit material, web sites promoting violence or terrorism, illegal use of controlled substances (drugs) and intolerance of other people/races/religions, etc.

Department Heads will determine which employees are given access to the Internet.

Careful Usage

Employee use of technology such as computer, Internet and Email, cellular phone, desktop phones, and digital equipment usage must be able to withstand public scrutiny without embarrassment to the City, its taxpayers, its clients, or its employees. Employees should use generally accepted standards of business conversation in all computer, Internet and Email usage. Employees should use good judgment in the type of message created and the tone and content of messages.

Data stored in any form using City equipment is considered City data. Such data is available to anyone authorized to see that data. While legal battles will continue on this issue for some time, expensive court settlements and case law provide some basic guidelines for using electronic mail (E-mail) **or any other form of storing data** as a City employee:

- ◆ Tact counts. If there is any doubt whether E-mail is the right medium for a message, use another form of communication.
- ◆ If you are a supervisor, never deliver a reprimand via E-mail.
- ◆ Never gossip or provide personal information about yourself or someone else or emotional responses to business memos.
- ◆ The use of insensitive language or derogatory, offensive, or insulting remarks is subject to discipline per City personnel policies and practices.
- ◆ The use of harassing language, including sexually harassing language or any remarks that may be misinterpreted as such is subject to discipline per City personnel policies and practices.
- ◆ E-mail is not confidential, and may be periodically reviewed.
- ◆ E-mail should be checked at least daily, unless the individual is away from the office.

In other words, use common sense and focus on City business.

Monitoring

The City of Hibbing reserves the right to monitor all uses of City technology, at the time of use, during routine post-use audits, and during investigations. The City also reserves the right to restrict access to various Internet sites and services.

The City may monitor City technology such as computers, Email and Internet systems and access messages and information stored on the system to:

- (1) Maintain the integrity and efficiency of the system.
- (2) Prevent and discourage unauthorized access and system misuse.
- (3) Retrieve business-related information.
- (4) Investigate reports of misconduct or misuse.
- (5) Reroute or dispose of undeliverable mail.
- (6) Respond to lawful requests for information.

Downloading and Email Attachments

Unless authorized by the City Administrator and supervisors, employees shall not download software from the Internet or receive software as an attachment to an Email message. If downloading or attaching is authorized, virus-scanning procedures as outlined by the City Administrator must be followed. Contact Compudyne for current virus scanning procedures.

Software Installation

Installation of software and downloading software from the Internet is not permitted on City of Hibbing computers without the approval from the City Administrator.

The City of Hibbing complies with all software copyrights and terms of all software licenses. City employees may not duplicate licensed software or related documentation. Any such duplication may subject employees and/or the City to both civil and criminal penalties under the United States Copyright Act. Personal software may be installed only at the direction of the City Administrator. City-owned software may not be loaded on to an external system unless the license agreement allows such and is approved by the City Administrator.

Virus Protection Software

The City of Hibbing has, within its network, software to identify and remove harmful viruses. It is the employee's responsibility to report any knowledge of viruses within the City's computer resources to the City Administrator immediately. It is in violation of City policy to knowingly introduce the City of Hibbing's computer resources to any risk of virus threat.

Users shall not change their system's configuration or take other steps to defeat virus protection devices or systems.

Individual employees are responsible for verifying that disks used or received from outside computers are scanned for viruses prior to their use in City computers.

Software and File Inspections

The City of Hibbing reserves the right to inspect any and all files stored in public and private areas of the network and on any computer in order to assure compliance with policy. If it is discovered that software was installed without prior approval, the City reserves the right to remove said software in order to protect its computer resources.

Employees may be subject to disciplinary action up to and including discharge for violating this or any other computer related policy.

In addition to authorized roles regarding software, the legal implications for improper handling of software can be significant:

According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as \$100,000 per works copies, and criminal penalties, including fines and imprisonment. The City of Hibbing does not condone the illegal duplication of software or any other form of criminal activity. Employees who engage in such activity are also subject to discipline using City personnel procedures.

Personal Use of City PC's

The City currently allows personal use of city PCs **only by city employees** during non-work hours when those PCs are not being used for City business. Employees are to provide their own paper and store their personal files on their own floppy disks. Floppy diskettes, CD-ROMs or other external data devices should be checked for viruses. City PC's is not to be used to manage any part of a private business or for political or criminal activity. No personal software or hardware is to be used on city PC's. Supervisors who determine that such uses are interfering with City business or are otherwise inconsistent with a positive public image may prohibit specific personal uses.

Other organizations will not use the City of Hibbing computers. Due to complex configuration of the City network and support issues, this would not be practically possible.

Portable Computer Usage

Portable personal computer(s) can be used for City business, outside of City facilities, after normal working hours provided these procedures are followed:

- ◆ The department the portable personal computer is located in has first priority.
- ◆ The supervisor must approve other employees' usage of the portable personal computer after normal working hours, unless the requesting employee is a Department or Division Head.

An employee may only use the City's portable personal computers for personal work within City facilities and in conformance with the Personal Use Policy.

Electronic Communication

Electronic communications can take a variety of forms such as telephone messages, voice mail, facsimile, electronic mail and similar computer-based documents.

Electronic communication is any message or data sent or received electronically. There are two main categories of electronic communication currently being utilized by the City: Electronic mail and voice mail. Electronic mail or e-mail is computer based and involves receiving and delivering some type of computer output (messages, letters, memos, spreadsheets, etc) via the city network and phone lines. Voice mail is a system whereby sounds, usually voices, are digitally recorded, transmitted, and stored. The City of Hibbing e-mail and voice mail systems are provided to facilitate City business communication among employees and other business associates. To assure the continued benefits that e-mail and voice mail makes possible, it is necessary for all employees using these forms of communication to adhere to uniform policies.

Proper Use

The e-mail and voice mail systems are City property and are intended for City business. The systems are not to be used for employee personal gain, illegal activities, or political activities. All data and other electronic messages within these systems are the property of the City of Hibbing. Limited and brief personal use of e-mail and voice mail is acceptable. Forwarding of non-business e-mails should be discouraged by supervisors since it lends itself to lower worker productivity.

Privacy

As a matter of routine, the City will not monitor e-mail or voice mail messages. However, the City, through its managers and supervisors, reserves the right to review the contents of employee's e-mail or voice mail files. Also, employees may not intentionally intercept, eavesdrop, record, alter, or receive other personal e-mail or voice mail messages without proper authorization.

Sensitive Issues

The e-mail and voice mail systems should not be used to transmit sensitive material such as personnel decisions, reprimands, or material which is confidential in nature. Avoid language that is insensitive, insulting, offensive, derogatory, harassing, or discriminatory. If you are in doubt whether electronic communication is the proper medium for a message, use another form of communication.

Checking E-mail and Voice mail

Both e-mail and voice mail should be checked at least daily. If the messages request a response the response should be sent as soon as possible. Receipt of an external message should be acknowledged immediately even if a subsequent response is required.

Deleting Messages

Generally, e-mail and voice mail messages are temporary communications, which are non-vital and may be discarded routinely. However, depending on the content of the message, it may be considered a more formal record and should be retained pursuant to a departments record retention schedule.

Junk mail (Spam)

Delete junk mail as soon as possible.

Graphics

Graphics require a lot of memory. Please limit distribution of graphics and if you receive messages with a graphic please delete it as soon as possible. Animations require large amounts of memory and should be avoided. If you receive animation it should be deleted as soon as possible.

Effective Date: _____

City Administrator

Date

Adopted: _____