CITY OF ROCHESTER
ORGANIZATIONAL POLICY

TECHNOLOGY

Scope

The City of Rochester provides hardware, software, programs, applications, templates, internal and external e-mail messages, facsimile (fax) messages, data, data files and voicemail messages developed or stored on city-owned, leased, or rented computer systems or storage media computer systems, voicemail systems, electronic mail ("e-mail"), and other information systems (hereinafter "City technology") to employees at City expense for their use in performing their duties for the City. This policy sets forth the City's guidelines for employee use of all City technology. This policy's goal is to avoid inappropriate use of systems, maintain appropriate security, avoid copyright violations and protect City-owned data and systems.

Ownership

All City technology systems are the property of the City of Rochester. The City retains the right to disclose City technology information to third parties without providing notice to employees. Employee use of City technology is not private. This includes, but is not limited to, the use of internal and external e-mail and Internet use. Use of passwords does not make files or data private. Passwords must be disclosed to supervisors upon request and may be bypassed by the City. E-mail messages are considered to be City property and may be retrieved from storage although the sender and receiver have deleted them. These messages may be used in disciplinary proceedings. By using City technology, employees consent to any monitoring of that technology that may take place.

Supervisors have the authority to inspect the contents of any City technology. The Information Systems Manager shall cause the extraction of stored e-mail messages when requested to do so by authorized supervisory personnel. Reasons for review include, but are not limited to, system hardware or software problems, general system failure, regular system maintenance, a lawsuit against the City, suspicion of a crime or violation of policy, or a need to perform work or provide a service when the employee is unavailable.

General Policy

Policy. It is the City's policy that City technology, like other City assets, is to be used for the benefit of the City. Use of City technology to violate other City policies is prohibited and may lead to disciplinary action up to and including termination. Any and all opinions made using these systems, whether implied or expressed, are those of the individual and not necessarily the opinions of the City or its officers.

Privacy. Employees should be aware that others might read messages created by City technology for a variety of valid reasons. Although this statement is true of many other types of City correspondence, the nature of e-mail messages in particular can lead one to forget or ignore the fact that e-mail cannot be considered the private property of the sender or recipient although passwords or encryption codes are used for security reasons.

E-mails Retained. Employees should also be aware that in the case of threatened or pending litigation involving the City, federal and state rules of civil procedure, statutes and caselaw require the City to collect and retain City employee-sent or City employee-received e-mail messages concerning the litigation until the litigation is finally resolved. These e-mail messages are subject to applicable federal or state civil discovery rules and the City, subject to any applicable privilege, must produce them upon demand. The City's failure to maintain these e-mail messages while litigation is pending subjects it to serious financial and litigation

consequences. Employees will be notified when their e-mail box becomes subject to such automated collection and retention. Employees are prohibited from tampering in anyway with the e-mail system in an attempt to avoid said collection and retention.

Electronic Profile Pictures. For purposes of identification, employees may upload a current personal headshot picture to their Microsoft 365 profile, which will be associated with their City Outlook and Teams account. Employees should use good judgement when selecting a picture and adhere to the following:

- The picture must be a headshot of the employee and shall not contain other people or images such as the employee's family members, cartoons, skylines, pets, scenery, or logos;
- The picture must be clear and unobstructed by optional accessories such as sunglasses or hats;
- Clothing must follow the City's Dress Standards and City-Funded Clothing Policy.

Personal Use. Pursuant to Section 13.45, subd. 3 of the Rochester Code of Ordinances, employees may make incidental and reasonable use of City technology for private purposes. Should employees make incidental use of City technology to transmit personal messages, these messages will be treated no differently than other messages. They may be accessed, reviewed, copied, deleted or disclosed. You should expect that a message may be disclosed to or read by others beyond its original intended recipients.

Authorized Uses. Supervisors or Department Heads may authorize the use of e-mail to send and receive messages and to subscribe to listserves from recognized professional organizations and entities relating to the City's official duties. All employees are authorized to use e-mail as they would us any other official City communication tool. E-mail communication is encouraged when it results in the most efficient or effective means of communications. The sender of e-mail messages must retain the primary responsibility for ensuring that the intended receiver receives the communication.

Use Subject to Authorization. The following uses require the employee's Department Head's written approval and Information System's concurrence:

- The use of hardware, related computer equipment and/or software for e-mail within the City network that the City did not purchase nor does not own.
- The reading of another employee's e-mail.
- The encryption of any e-mail message unless specifically authorized to do so and without depositing the encryption key with the LAN administrator or the employee's immediate supervisor. The fact that an employee is allowed to encrypt e-mail does not mean that the e-mail is intended for personal communication, nor does it mean that encrypted e-mail messages are the employee's private property.

Prohibited Uses

The following actions are prohibited:

- Intercepting, eavesdropping, recording or altering of another person's e-mail message.
- Adopting the identity of another person on any e-mail message, attempting to send e-mail anonymously, or using another person's password without their permission.
- Misrepresenting your affiliation on any e-mail message.
- Using e-mail for any commercial promotional purpose including personal messages offering to buy or sell goods or services.
- Sending or receiving software in violation of copyright law.

- Using City technology for a personal for-profit commercial purpose, or to communicate any material of an obscene or derogatory nature.
- Displaying, printing or transmitting sexually explicit images, messages or cartoons.
- Displaying, printing or transmitting racial, sexual or ethnic slurs, comments, derogatory jokes or cartoons, or anything that might be construed as harassment, abusive, offensive or disrespectful of others. This includes anything that fosters a hostile work environment or perpetuates discrimination on the basis of race, creed, color, age, religion, sex, marital status, status with regard to public assistance, national origin, physical or mental disability or affectional preference.
- Use of the City's Internet mail address for participation in personal or non-City business related e-mail lists.
- Sharing your user ID or password with anyone without specific permission to do so granted by the Department Head or City Administrator. If access to City technology is needed by someone who does not have access, the Information Systems manager should be contacted so properly restricted access is granted. If this access is temporary, the duration of access needs to be communicated at the time of the request.
- Attempting to gain unauthorized access to internal or external computer systems.
- Attempting to decrypt system or user passwords.
- Unauthorized copying of system files or software programs.
- Unauthorized deletion of e-mail messages and data records or files.
- Unauthorized printing, forwarding or disclosing confidential information.
- Attaching any form of electronic equipment device (e.g. thumb drive, iPod or other MP3 player, smartphone, etc.) to City equipment without IT approval.
- Attaching any form of electronic equipment (e.g. laptop, portable network drive, server, other computer, tec.) to the City network without IT approval.

Confidential Information

Minnesota law requires all employees to protect the integrity of the City's confidential information as well as the confidentiality of others. Employees must exercise a greater degree of caution in transmitting confidential information on the City technology system than with other communication means because of the reduced effort required to redistribute such information. Confidential information should never be transmitted or forwarded to other employees inside the City or anyone outside of the City who do not have a need to know the information. To reduce the chance that confidential information may be sent inadvertently to the wrong person, avoid misuse of distribution lists when sending information and make sure any lists are current.

If you are unsure whether information is confidential, you must consult with the City Attorney's Office.

Here is a partial list of some types of information which may be confidential (this is not an exhaustive list):

- Information from a person's personnel file, including home address, phone numbers and social security numbers.
- Information relating to any pending criminal or civil litigation, judicial or administrative proceeding.
- Information which would give a competitive advantage to one competitor or bidder over another.
- Information relating to the location or price of property the City might buy.
- Private correspondence of elected officials.
- Trade secrets, commercial or financial information of outside businesses.
- Information related to the regulation of financial institutions of securities.

- Information or communication from the City Attorney's Office or other City legal counsel.

E-mail messages that contain confidential information may, but is not required to, have a confidentiality legend in all capital letters at the top of the message in a form similar to the following:

THIS MESSAGE CONTAINS CONFIDENTIAL INFORMATION
OF THE CITY OF ROCHESTER.
UNAUTHORIZED USE OR DISCLOSURE IS PROHIBITED.

Since copies of e-mail may be placed on back up or other systems you do not control, and may be accessed by Information System personnel or others without a need to know the information, e-mail may be an inappropriate method to communicate certain types of confidential information.

Backing Up/Deleting Files

The Information Systems Department backs up all data except for any files that are stored on the hard drives of employee's computers. Employees are expected to store important work-related data on their network drive to avoid loss through hardware failure. Employees are also expected to delete old files regularly in compliance with the City's record retention schedule to help maintain adequate system storage capacity.

Copying Data/Programs Onto City Computers

All data files, e-mail attachments, and software programs must be checked by virus detection software before copying them onto the City's computer system. This includes downloading software from the Internet, remote bulletin boards and any on-line services.

Checking Out City Technology

When employees check out portable equipment such as laptop computers, VCRs, and computer projection units, they are expected to provide appropriate common sense protection against theft, accidental breakage, environmental damage and other risks. Desktop computers and attached devices are not to be removed from City buildings.

Miscellaneous Considerations for E-mail Messages

E-mail is a valuable form of communication which can help the City improve its quality of service. However, employees should consider the following when considering whether a message is appropriate for e-mail communication:

- Avoid making a statement in an e-mail message about someone if you would not make the statement face-to-face with the person or write it in a formal memo.
- Avoid making a statement in an e-mail message which may be perceived as being ill-considered, uninformed or offensive.
- Avoid using e-mail if a more time or cost-effective communication is available (for instance, when a telephone conversation would be faster).
- Avoid using e-mail as a substitute for manager-subordinate face-to-face communications.
- Avoid using e-mail for the purpose of evaluating one's job performance.

Copyright Infringement

Most computer software and programs are copyrighted, and it is illegal to make multiple copies. Employees may only copy and use software according to the software license agreement.

The ability to attach a document to an e-mail message for distribution greatly enhances the risk of copyright infringement. A user can be liable for the unauthorized copying and distribution of copyrighted material through the e-mail system. Accordingly, you should not copy and distribute through the e-mail system any copyrighted material of a third party (such as software, database files, documentation, articles, graphics files and down-loaded information) unless you confirm in advance from appropriate sources that the City has the right to copy or distribute such material. Any questions concerning copyright information should be directed to the City Attorney's Office.

E-Mail Message Retention – 60 Days

Normally e-mail messages are transitory, of short-term interest, and are considered incidental and non-vital communications. As such, normal e-mail messages are not subject to specific record retention schedules and should be disposed of immediately after action or review. E-mail is not an official communication of the City and must not be used for transmitting information that is part of the official record. In the event that an e-mail message occurs that relates to the transaction of official City business, the message should be reduced to print form or other City-approved archival format (electronic, optical, or otherwise), and should be retained in accordance with applicable retention schedules. Otherwise, Information System staff will delete all messages after 60 days whether opened or unopened. The only exception to this retention limit is for legal discovery as noted in under "General Policy," Item 3., above.

Unauthorized Access

All suspected intrusions to the City's network systems by unauthorized persons or employees are to be reported immediately to the Department Head and Information Systems personnel.

Penalties/Consequences

Violations of this policy will result in disciplinary measures that may include reprimands, suspension of some or all computer usage privileges, and termination. All City technology messages are subject to all applicable state and federal laws. In addition, violations of this policy or misuse of the City technology system that are of a criminal nature may be referred for criminal prosecution.

Revised and approved by the City Administrator:

Steve Rymer
May 19, 2020

Revised/Adopted 10/15/07, Revised/Adopted 6/7/10, Revised 05/07/2020