CITY OF RACINE ELECTRONIC COMMUNICATIONS AND E-MAIL POLICY

Issue Date:	Revision Update(s):	Total Pages:
Adopted January 1, 2015	February 21, 2018 (format only)	10

Policy Source:
City of Racine, Human Resources Department

Special Instructions: This policy applies to all elected officials and employees of the City of Racine. In addition to the provisions of this policy, such officials and employees are required to comply with State and local traffic laws and City/Development Safety and Work Rules.

I. ELECTRONIC COMMUNICATION

A. PURPOSE

To better serve our citizens and give our workforce the best tools to do their jobs, the City of Racine continues to adopt and make use of new means of communication and information exchange. This means that many of our employees have access to one or more forms of electronic media and services, including, but not limited to, computers, e-mail, telephones, cellular telephones, pagers, voice mail, fax machines, external electronic bulletin boards, wire services, on-line services, the Internet, and the World Wide Web.

The City of Racine encourages the use of these media and associated services because they can make communication more efficient and effective and because they are valuable sources of information. However, all employees and everyone connected with the City should remember that electronic media and services provided by the City are City property and their purpose is to facilitate and support City business. No expectation of privacy in regards to use of the City's electronic communication systems should be expected by the employee in any respect related to accessing, transmitting, sorting or communicating information via the system.

This policy cannot lay down rules to cover every possible situation. The purpose of this policy is to express the City of Racine's philosophy and set forth general guidelines governing the use of electronic media and services. By adopting this policy, it is the City's intent to ensure the electronic communication systems are used to their maximum potential for business purposes and not used in a way that is disruptive, offensive to others, or contrary to the best interest of the City of Racine.

1. The following procedures apply to all electronic media and services that are:

a. Accessed on or from City premises;
b. Accessed using the City's computer equipment or via the City's paid access methods; or
c. Used in a manner that identifies the individual as acting for or on behalf of the City of Racine; or in any way identifies the City of Racine.

2. Organizations affected:

   This policy applies to all of the departments, offices, boards, commissions, committees, employees and contracted and consulting resources of the City of Racine.

B. POLICY

It is the policy of the City of Racine to follow this set of procedures for the use of electronic communication media and services.

References:
Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510 - 2711); Wis. Stats. §947.0125.

C. PROCEDURES

1. Access and Authority

a. Each Department Head shall determine which employees in their department shall have access to the various media and services, based on business practices and necessity and which shall have authority to communicate on behalf of the department.

b. The provisions of this Policy shall apply to the use of City owned/provided equipment and/or services from home or other locations off City premises. City owned equipment (e.g. laptops) may be removed from City premises solely for City work related purposes pursuant to prior authorization from the Department Head.

2. Prohibited Communications

a. Electronic media cannot be used for knowingly transmitting, retrieving or storing any communication that is:

i. Personal business on City time (e.g. sports pools, games, shopping, correspondence, or other non-business-related items/documents), except as otherwise allowed under #3 below;
ii. Discriminatory or harassing;
iii. Derogatory to any individual or group;
iv. Obscene as defined in Wis. Stats. § 944.21;
v. Defamatory or threatening; or
vi. Engaged in for any purpose that is illegal or contrary to the City's policy or business interests.

b. For the protection, integrity and security of the City's System, electronic media shall not be used to download or transfer software, unless authorized by the Information Systems Director.

3. Personal Use

a. Except as otherwise provided, electronic media and services are provided by the City for employees' business use during City time. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal non-business purposes is permitted as set forth below:

i. Personal use is limited to breaks, lunch or immediately before/after work;
ii. Personal use must not interfere with the productivity of the employee or his or her co-workers;
iii. Personal use does not involve any prohibited activity (see Section B, b-f);
iv. iv. Personal use does not consume system resources or storage capacity on an ongoing basis;
v. Personal use does not involve large file transfers or otherwise deplete system resources available for business purposes.

b. City telephones and cellular phones are to be used for City business. However, brief, limited personal use is permitted during the work day. Personal long distance calls are only permitted with the use of a personal 1-800 calling card, or with the understanding that such calls must be reimbursed to the City, as per policies set forth in the City of Racine Employee Handbook.

c. Employees should not have any expectation of privacy with respect to personal use of the City's electronic media or services.

4. Access to Employee Communications

a. Electronic information created and/or communicated by an employee using e-mail, word processing, utility programs, spreadsheets, voice mail, telephones, Internet and bulletin board systems, desktop faxes, and similar electronic media may be accessed and monitored by the City of Racine. The City respects its employees' desire to work without surveillance. However, the City of Racine reserves and intends to exercise the right, at its discretion, to review, monitor, intercept, access, and disclose all messages created, received or sent over the electronic communication systems for any purpose including, but not limited to: cost analysis; resource allocation; optimum technical management of information resources; and detecting use which is in violation of City policies or may constitute illegal activity.

Disclosure will not be made except when necessary to enforce the policy, as permitted or required under the law, or for business purposes.

b. Any such monitoring, intercepting and accessing shall observe any and all confidentiality regulations under Federal and State laws.

5. Security/Appropriate Use

a. Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by the Information Systems Director, employees are prohibited from engaging in, or attempting to engage in:

i. Monitoring or intercepting the files or electronic communications of other employees or third parties;
ii. Hacking or obtaining access to systems or accounts they are not authorized to use;
iii. Using other people's log-ins or passwords; and

iv. Breaching, testing, or monitoring computer or network security measures.

b. No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

c. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

d. Anyone obtaining electronic access to other organizations', business', companies', municipalities' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify, or forward copyrighted materials except as permitted by the copyright owner.

Employees must understand that the unauthorized use or independent installation of non-standard software or data may cause computers and networks to function erratically, improperly, or cause data loss. Therefore, before installing any new software or data, users should seek assistance of the Information Systems Department. Users must never install downloaded software to networked storage devices without the assistance and approval of appropriate personnel.

Most of the City's computing facilities automatically check for viruses before files and data which are transferred into the system from external sources are run or otherwise accessed. On computers where virus scanning takes place automatically, the virus scanning software must not be disabled, modified, uninstalled, or otherwise inactivated. If you are uncertain as to whether the workstation you are using is capable of detecting viruses automatically, or you are unsure whether the data has been adequately checked for viruses, you should contact the Information System Department's Help Desk.

Anyone receiving an electronic communication in error shall notify the sender immediately. The communication may be privileged, confidential and/or exempt from disclosure under applicable law. Such privilege and confidentiality shall be respected.

6. Encryption

Employees should not assume electronic communications are totally private. Employees with a business-need to encrypt messages (e.g. for purposes of safeguarding sensitive or confidential information) shall submit a written request to their supervisor and their Administrative Manager. When authorized to use encryption by their supervisor and their Administrative Manager, employees shall use encryption software supplied to them by the Information Systems Department. Employees who use encryption on files stored on a City's computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

7. Participation in on-line forums

a. Employees should remember that any messages or information sent on City provided facilities to one or more individuals via an electronic network (for example: Internet mailing lists, bulletin boards, and on-line services) are statements identifiable and attributable to the City of Racine.

b. The City of Racine recognizes that participation in some forums might be important to the performance of an employee's job. For instance, an employee might find the answer to a technical problem by consulting members of a newsgroup devoted to the technical area.

c. Employees shall include the following disclaimer in all of their postings to public forums:

"The views, opinions, and judgments expressed in this message are solely those of the author. The message contents have not been reviewed or approved by the City Attorney's Office".

d. Employees should note that even with a disclaimer, a connection with the City of Racine exists and a statement could be imputed legally to the City. Therefore, employees should not rely on disclaimers as a way of insulating the City from the comments and opinions they contribute to forums. Instead, employees must limit their discussion to matters of fact and avoid expressing opinions while using the City's systems or provided account. Communications must not reveal confidential information and must not otherwise violate this or other City policies.

e. Employees must receive authorization from their Department Heads prior to participating in an on-line forum. The employees shall be required to review the provisions of this section before they receive such authorization.

8. Policy Violations

Employees who abuse the privilege of City facilitated access to electronic media or services risk having the privilege removed for themselves and possibly other employees, are subject to discipline, up to and including termination, and may be subject to civil liability and criminal prosecution.

II. E-MAIL POLICY

A. PURPOSE

The City of Racine provides certain employees with systems to send and receive electronic mail (e-mail) so they can work more productively. E-mail gives employees a useful way to exchange ideas, share files, and keep in touch with colleagues, whether they are located in the next room, another City building, or thousands of miles away.

The City of Racine's e-mail system is a valuable business asset. The messages sent and received on the e-mail system, like memos, purchase orders, letters, or other documents created by employees in the course of their workday, are the property of the City of Racine and may constitute public records. This policy explains rules governing the appropriate use of e-mail and sets out the City's rights to access messages on the e-mail system. No expectation of privacy in

regards to use of the City's e-mail system should be expected by the employee in any respect related to accessing, transmitting, sorting or communicating information via the system.

1. Organizations affected:

This policy applies to all City departments, divisions, offices, boards, commissions, committees, employees and contracted and consulting resources.

B. POLICY

It is the policy of the Governing Unit to follow this set of procedures for the use of the Governing Unit's e-mail system.

References:

Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510 - 2711); Wis. Stats. §19.21; Wis. Stats. §947.0125.

C. PROCEDURES

1. Access to employee e-mail

a. Employees should not have any expectation of privacy with respect to messages or files sent, received, or stored on the City's e-mail system. E-mail messages and files, like other types of correspondence and City documents, can be accessed and read by authorized employees or authorized individuals outside the City. The City reserves the right to monitor, review, audit, intercept, access and disclose all messages created, received or sent over the e-mail system. Information contained in the e-mail system will only be disclosed to the extent permitted by law, for business purposes, or as needed to enforce the policy. Authorized access to employee e-mail by other employees or outside individuals includes, but is not limited to, the following:

i. Access by the Information Systems Department during the course of system maintenance or administration;
ii. Access approved by the employee, the employee's supervisor, or Administrative Manager when there is an urgent business reason to access the employee's mailbox - for example, if an employee is absent from the office and the supervisor has reason to believe that information relevant to the day's business is located in the employee's mailbox;
iii. Access approved by the employee's supervisor, the Administrative Manager, or the City Administrator when there is reason to believe the employee is using e-mail in violation of the City's policies;
iv. Access approved by the City Administrator or the City Attorney in response to the City's receipt of a court order or request from law enforcement officials for disclosure of an employee's e-mail messages.

b. Except as otherwise noted herein, e-mail should not be used to communicate sensitive or confidential information. Employees should anticipate that an e-mail message might be disclosed to or read by individuals other than the intended recipient(s), since messages can be easily forwarded to other individuals. In addition, while the City endeavors to maintain the

reliability of its e-mail system, employees should be aware that a variety of human and system errors have the potential to cause inadvertent or accidental disclosures of e-mail messages.

c. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message.

d. Employees should understand that electronic mail is a written form of communication, just like a paper letter. Though electronic mail is relatively spontaneous compared with regular mail, employees should take care to use the same level of discretion and forethought before executing electronic messages.

2. Passwords

Each user accesses the e-mail system by means of a personal log-in name and password, which will be selected by the employee and kept on file with the Department Head and the Information Systems Department.

a. Passwords are intended to keep unauthorized individuals from accessing messages stored on the system. From a systems perspective and from the perspective of an e-mail recipient, passwords also establish the identity of the person sending an e-mail message. The failure to keep passwords confidential can allow unauthorized individuals to read, modify, or delete e-mail messages; circulate e-mail forgeries; and download or manipulate files on other systems.

b. The practice of using passwords should not lead employees to expect privacy with respect to messages sent or received. The use of passwords for security does not guarantee confidentiality. (See "Access to Employee E-mail").

c. Passwords should never be given out over the phone, included in e-mail messages, posted, or kept within public view.

d. Employees are prohibited from disclosing their password, or those of any other employee, to anyone who is not an employee of the City. Employees also should not disclose their password to other employees, except when required by an urgent business matter (see Section C. 1. a. ii. of this policy).

3. Personal Use

a. The City of Racine allows limited, occasional, or incidental personal use of its e-mail system during lunch, breaks or immediately before or after work, subject to the following conditions and restrictions:

b. Personal use must not:

i. Involve any prohibited activity (see #4 below);

ii. Interfere with the productivity of the employee or his or her co-workers;

iii. Consume system resources or storage capacity on an ongoing basis; or

iv. Involve large file transfers or otherwise deplete system resources available for business purposes.

c. Employees should not have any expectations of privacy with respect to personal e-mail sent or received on the City's e-mail system. Employees should delete personal messages as soon as they are read or replied to. Employees should not store copies of the personal messages they have sent. Because e-mail is not private, employees should avoid sending personal messages that are sensitive or confidential.

4. Prohibited Activities

a. Employees are strictly prohibited from sending e-mail or otherwise using the e-mail system in connection with any of the following activities:

i. Engaging in personal business or entertainment on the City's time;
ii. Engaging in illegal, fraudulent, or malicious activities;
iii. Engaging in the unlawful use of the e-mail system as set forth in Section 947.0125 of the Wisconsin Statutes (Unlawful use of computerized communication systems);
iv. Sending or storing offensive, disruptive, obscene, or defamatory material. Materials which are considered offensive include, but are not limited to: any materials which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, race, creed, color, sex, ancestry, religious or political beliefs, marital status, national origin or disability;
v. Annoying or harassing other individuals;
vi. Using another individual's account or identity without explicit authorization;
vii. Attempting to test, circumvent, or defeat security or auditing systems, without prior authorization;
viii. Accessing, retrieving or reading any e-mail messages sent to other individuals, without prior authorization from the Information Systems Department; or
ix. Permitting any unauthorized individual to access the City's e-mail system.

5. Confidential Information

a. All employees are expected and required to protect the City of Racine's confidential information. Employees shall not transmit or forward confidential information to outside individuals or companies without the permission of their supervisor and the City Administrator. See #7 Encryption.
b. The City also requires its employees to use e-mail in a way that respects the confidential and proprietary information of others. Employees are prohibited from copying or distributing copyrighted material - for example, software, database files, documentation, or articles using the e-mail system.

6. Record Retention

a. The same rules which apply to record retention for other City documents apply to e-mail. As a general rule, e-mail is a public record whenever a paper message with the same content would be a public record.
b. The specific procedure to be followed with respect to the retention of e-mail records is contained in Section 3, E-Mail Record Retention Policy.

7. Encryption

Encrypting e-mail messages or attached files sent, stored, or received on the Governing Unit's e-mail system is prohibited except where explicitly authorized. Employees are prohibited from using or installing any encryption software without prior permission from the Information Systems Director. Employees with a business need to encrypt messages should submit a written request to their supervisor and their Administrative Manager. When authorized to use encryption by their supervisor and their Administrative Manager, employees shall use encryption software

supplied to them by the Information Systems Department. Employees who use encryption on e-mail stored on a City computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all the passwords and/or encryption keys necessary to access the e-mail.

8. E-mail Policy Violations

Employees violating the City of Racine's e-mail policy are subject to discipline, up to and including termination. Employees using the e-mail system for defamatory, illegal, or fraudulent purposes and employees who break into unauthorized areas of the City's computer system also are subject to civil liability and criminal prosecution.

III. E-MAIL RECORD RETENTION POLICY

A. PURPOSE

The purpose of this policy is to emphasize that certain types of e-mail as defined in Wis. Stats. §19.32(2) are public records. The same rules which apply to record retention and disclosure for other Governing Unit documents apply to such records. This policy applies to all of the departments, divisions, offices, boards, commissions, committees, employees and contracted and consulting resources of the City of Racine.

B. POLICY

It is the policy of the Governing Unit to follow this set of procedures for e-mail record retention.

References:
Wis. Stats. §§16.612, 19.21 et. seq., 19.32 and 19.33.

C. PROCEDURES

1. Nature of e-mail records
As a general rule, e-mail is a public record whenever a paper message with the same content would be a public record. See Wis. Stats. §19.32(2) for definition of a record.

2. Components of an e-mail record
The e-mail record is defined to include the message, the identities of the sender and all recipients, the date, and any non-archived attachments to the e-mail message. Any return receipt indicating the message was received by the sender is also considered to be part of the record.

3. Saving and indexing e-mail records
Initially the custodian (that officer, department head, division head, or employee of the City who keeps or is in possession of an e-mail) bears the responsibility for determining whether or not a particular e-mail record is a public record which should be saved and ensuring the record is properly indexed and forwarded for retention as a public record. E-mail which is subject to records retention must be saved and should be indexed so that it is linked to the related records in

other media (for example, paper) so that a complete record can be accessed when needed. E-mail records to be retained shall be archived to an archival media, network drive or printed out and saved in the appropriate file. Any officer, department head, division head, or employee of the City may request assistance from the City Attorney's Office in determining whether an e-mail is a public record.

4. Responsibilities for e-mail records management

a. Legal Custodian. E-mail records of a City department having custody of records shall be maintained by the designated Legal Custodian, pursuant to City policy.

b. Information Systems Director. If e-mail is maintained in an on-line data base, it is the responsibility of the Information Systems Department to provide technical support for the Legal Custodian as needed. When equipment is updated, the Information Systems Department shall ensure that the ability to reproduce e-mail in a readable form is maintained. The Information Systems Director shall assure that e-mail programs are properly set up to archive e-mail.

5. Public access to e-mail records

If a Department receives a request for release of an e-mail public record, the Legal Custodian of the record shall determine if it is appropriate for public release, in whole or in part, pursuant to law, consulting the City Attorney's Office, if necessary. As with other records, access to or electronic copies of disclosable records shall be provided within a reasonable time.

6. Violation

Employees violating this policy are subject to discipline up to and including dismissal. In addition, violations of this policy may be referred for civil and/or criminal prosecution, where appropriate.