

E-Mail Policy	Information Technology	1300
	1312	1 – 7
		02/06/98
		10/21/14

1.0 PURPOSE:

The City of West Allis (the "City") 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'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 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.

2.0 ORGANIZATIONS AFFECTED:

This policy applies to all City of West Allis departments, divisions, offices, boards, commissions, committees and City employees.

3.0 POLICY:

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

4.0 REFERENCES:

Electronic Communications Privacy Act of 1986 and its exceptions; Wis. Stats. §19.21; Wis. Stats. §947.0125.

5.0 PROCEDURES:

5.1 ACCESS TO EMPLOYEE E-MAIL

5.1.1 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 review, audit, intercept, access and disclose all messages created, received or sent over the e-mail system for any purpose. The contents of e-mail properly obtained for legitimate business purposes, may be disclosed within the City without the permission of the employee. Authorized access to employee e-mail by other employees or outside individuals includes, but is not limited to, the following:

- 1.) Access by the systems administration staff during the course of system maintenance or administration;
- 2.) Access approved by the employee, the employee's supervisor, or an officer of the City 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;
- 3.) Access approved by the employee's supervisor, the City's Personnel Division, or an officer of the City when there is reason to believe the employee is using e-mail in violation of the City's policies;
- 4.) Access approved by the City's Personnel Division or the City Attorney's Office 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.

5.1.2 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.

5.1.3 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.

5.2 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.

5.2.1 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.

5.2.2 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 Section 5.1, "Access to Employee E-mail").

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

5.2.4 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 5.1.1(2) of this policy).

5.3 PERSONAL USE

5.3.1 The city allows limited, occasional, or incidental personal use of its e-mail system during lunch or break times, subject to the following conditions and restrictions:

- 1.) Personal use must not:
 - a.) Involve any prohibited activity (see Section 5.4);
 - b.) Interfere with the productivity of the employee or his or her co-workers;
 - c.) Consume system resources or storage capacity on an ongoing basis; or
 - d.) Involve large file transfers or otherwise deplete system resources available for business purposes.
- 2.) 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.

5.4 PROHIBITED ACTIVITIES

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

- 1.) Engaging in personal business or entertainment on City time;
- 2.) Engaging in illegal, fraudulent, or malicious activities;
- 3.) 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);
- 4.) 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;
- 5.) Annoying or harassing other individuals;
- 6.) Using another individual's account or identity without explicit authorization;
- 7.) Attempting to test, circumvent, or defeat security or auditing systems, without prior authorization;

- 8.) Accessing, retrieving or reading any e-mail messages sent to other individuals, without prior authorization; or
- 9.) Permitting any unauthorized individual to access the City's e-mail system.

5.5 CONFIDENTIAL INFORMATION

- 5.5.1 All employees are expected and required to protect the City's confidential information. Employees shall not transmit or forward confidential information to outside individuals or companies without the permission of their supervisor and the Systems Administrator. See Section 5.7, Encryption.
- 5.5.2 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.

5.6 RECORD RETENTION

- 5.6.1 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.
- 5.6.2 The specific procedures to be followed with respect to the retention of e-mail records is contained in the City's E-Mail Record Retention Policy. The E-Mail Record Retention Policy shall be reviewed by all employees in conjunction with this E-Mail Policy and it shall be incorporated herein as if fully set forth.

5.7 ENCRYPTION

Encrypting e-mail messages or attached files sent, stored, or received on the City'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 City's Systems Administrator. Employees with a business need to encrypt messages should submit a written request to their supervisor and the Systems Administrator. When authorized to use encryption by their supervisor and the Systems Administrator, employees shall use encryption software supplied to them by the Systems Administrator. 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.

5.8 E-MAIL POLICY VIOLATIONS

Employees violating the City'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.

5.9 STANDARD DISCLAIMER

All outbound e-mails shall contain the standard disclaimer specified by the City Attorney's Office as listed in the attached "City of West Allis Disclaimer." This disclaimer will be automatically appended to all outgoing emails by the City's e-mail server.

E-MAIL AND ELECTRONIC COMMUNICATIONS POLICIES

EMPLOYEE NOTICE

As an employee of the City of West Allis (the "City"), I recognize and understand that the City's electronic communication systems are provided for conducting the City's business. However, City policy does permit some limited, occasional, or incidental personal use of the equipment and services under certain circumstances. I understand that all equipment, software, messages and files are the exclusive property of the City. I agree not to use the electronic communication systems in a way that is disruptive, offensive, or harmful to others or to the City. I agree not to use pass codes, access a file or retrieve any stored communication other than where authorized. I agree not to copy, send or receive confidential information without prior authorization from my immediate supervisor and the Systems Administrator.

I am aware that the City reserves and will exercise the right to review, audit, intercept, access and disclose all matters on the City's electronic communications systems at any time. I am aware that the City may exercise these rights with or without employee notice, and that such access may occur during or after working hours. I am aware that use of a log-in name and password do not guarantee confidentiality, guarantee privacy or restrict the City's right to access electronic communications. I am aware that violations of this policy may subject me to disciplinary action, up to and including discharge from employment, as well as civil and/or criminal liability.

I acknowledge that I have read and that I understand the City's policies regarding e-mail and electronic communications. I also acknowledge that I have read and that I understand this notice.

Signature of Employee

Date

POLICY REMINDER

Use of electronic communication systems is controlled by the City's E-mail and Electronic Communication Policies. These systems are provided for **BUSINESS USE**. However, City policy does permit some limited, occasional, or incidental personal use under certain circumstances. The City has the **RIGHT TO MONITOR** all messages and Internet activities. Employees have **NO RIGHT TO PRIVACY** when using these systems. Misuse of the systems may subject employees to discipline up to and including termination and/or loss of access privileges. If you have not reviewed and signed an acknowledgement form for the City's E-mail and Electronic Communication Policies, you may not access these systems.

**PRESSING "OK" SIGNIFIES YOU HAVE READ AND ACKNOWLEDGE THE
CITY'S E-MAIL AND ELECTRONIC COMMUNICATION POLICIES**

CITY OF WEST ALLIS DISCLAIMER

General

The City of West Allis is subject to Wisconsin Statutes relating to public records. Email sent or received by City employees are subject to these laws. Unless otherwise exempted from the public records law, senders and receivers of City email should presume that the email are subject to release upon request, and to state record retention requirements.

This email and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to which they are addressed. The recipient should check this email and any attachments for the presence of viruses. The City of West Allis accepts no liability for any damage that may be caused by a virus that may be inadvertently transmitted by this email.

If you have received this email in error, please destroy it and notify the sender immediately.

Regarding Contract Language

Nothing in this message or its contents should be interpreted to authorize or conclude a binding agreement or contract between the City of West Allis and the recipient of this email and its attachments without the express written confirmation by a City of West Allis employee who is authorized to enter into lawful contracts.

Regarding Legal Advice

If this email is from the City of West Allis and is providing legal advice, it may contain information which is privileged, confidential, and protected by attorney client or attorney work product privileges. If you are not the intended addressee, note that any disclosure, copying, distribution, or use of the contents of this message is prohibited.

Regarding Tax Advice

Pursuant to Circular 230 promulgated by the Internal Revenue Service, if this email, or any attachment hereto, contains advice concerning any federal tax issue or submission, please be advised that it was not intended or written to be used, and that it cannot be used, for the purpose of avoiding federal tax penalties unless otherwise expressly indicated. 31 CFR Part 10, § 10.35.

Regarding Trade Secrets

The information in the email may include trade secrets or privileged or otherwise confidential information. Unauthorized review, forwarding, printing, copying, distributing, or using such information is strictly prohibited and may be unlawful.