

**ARTICLE XXIX: ELECTRONIC COMMUNICATION AND INFORMATION SYSTEMS
POLICY**

SECTION 1 - ELECTRONIC COMMUNICATION

PURPOSE

To better serve our citizens and give our workforce the best tools to do their jobs, the City of Manitowoc (“City”) continues to adopt and make use of new means and methods of communication and information exchange. Many of our employees, officers, elected officials, boards, commissions, committees, contracted and consulting services 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, the Intranet, and the World Wide Web.

The City encourages the use of these media and associated services because they make communication more efficient and effective and because they are valuable sources of information. However, all employees, officers, elected officials, boards, commissions, committees, contracted and consulting services 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 regard to use of the City’s electronic communication systems shall be expected by any employee, officer, elected official, board, commission, committee, contracted and consulting service in any respect related to accessing, transmitting, sorting, use or communicating information via communication systems.

This policy cannot provide a rule to cover every possible situation. The purpose of this policy is to express the City’s philosophy and set forth 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 prohibited, disruptive, offensive to others, or contrary to the best interest of the City.

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

- Accessed on or from City premises;
- Accessed using City computer equipment, virtual private network (VPN), telephones, cell phones, pagers, fax machines, e-mail, Internet and World Wide Web, or via City paid access methods; or
- Accessed by any means which identifies the individual as acting for or on behalf of the City or in any way identifies the City.

ORGANIZATIONS AFFECTED:

This policy applies to the entire City government including its departments, offices, officers,

elected officials, boards, commission, committees, City employees and contracted and consulting services (e.g. MPU I.T. department).

POLICY:

It is the policy of the City to follow this set of procedures for the use of electronic communication media and services of whatever kind and nature, currently in existence and use and hereafter placed in service by the City or any electronic communication media or service personally owned and used for City of Manitowoc business purposes.

REFERENCES:

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

PROCEDURES:

Access and Authority

1. 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 City. A written document listing those who shall have access and the means of access authorized shall be maintained by the Department Head.
2. The provisions of this Policy shall apply to the use of City owned/provided equipment or the use of computer or portable memory devices owned by an employee, officer or elected official for conducting City business and/or services from home or other locations off City premises. City-owned equipment (e.g. lap tops) may be removed from City premises solely for City work related purposes pursuant to prior authorization from the Department Head.

Prohibited Communications

3. Electronic media shall not be used for knowingly transmitting, retrieving or storing any communication that is:
 - a. For personal use on City time (e.g. sports, pools, games, shopping, jokes, cartoons, correspondence or other non-business-related items/documents), except as otherwise allowed under “Personal Use”;
 - b. Discriminatory or harassing;
 - c. Derogatory to any individual or group;
 - d. Obscene as defined in Wis. Stat. §944.21;

- e. Defamatory or threatening; or
- f. Engaged in for any purpose that is illegal or contrary to the City's policy or business interests

Personal Use

1. 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 nonbusiness purposes is permitted as set forth below:
 - a. Personal use is limited to breaks, lunch or immediately before/after work;
 - b. Personal use must not interfere with the productivity of the employee or his or her co-workers;
 - c. Personal use does not involve any prohibited activity (see Section 3 above);
 - d. Personal use does not involve large file transfers or otherwise deplete system resources available for business purposes.
2. 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 using land lines are prohibited except in the case of emergency as per policies set forth in the City Employee Policy Manual.
3. Employees shall have no expectation of privacy with respect to personal use of the City's electronic media or services.

Access to Employee Communications

1. Electronic information created, but not limited to, and/or communicated by an employee, officer, elected official, board, commission, committee, contracted and consulting service using e-mail, word processing, utility programs, spreadsheets, voice mail, telephones, Internet and bulletin board systems, faxes, and similar electronic media may be accessed and monitored by the City. The City respects its employees', officers', elected officials', boards', commissions', committees', contracted and consulting services' desire to work without surveillance. However, the City reserves and intends to exercise the right, at its sole 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; public record disclosures; 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.

2. Any such monitoring, intercepting and accessing shall observe any and all confidentiality regulations under federal and state laws.

Security/Appropriate Use

1. Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services shall respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by the City Attorney and Human Resources Director and at least two of the following: the employee's Department Head, the Mayor, Library Board President, or Council President they are prohibited from engaging in, or attempting to engage in:
 - a. Monitoring or intercepting the files or electronic communications of other employees, officers, elected officials, boards, commissions, committees, contracted and consulting services or third parties;
 - b. Hacking or obtaining access to systems or accounts they are not authorized to use;
 - c. Using other people's log-ins or passwords without that person's consent; and
 - d. Breaching, testing or monitoring computer or network security measures.
2. 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.
3. Electronic media and services shall not be intentionally 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.
4. Anyone obtaining electronic access to other organizations', business', companies', municipalities' or individual's materials shall respect all copyrights and cannot copy, retrieve, modify, or forward copyrighted materials except as permitted by the copyright owner.

Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services 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 and receive permission from the Electronic Data Processing Department. User must never install downloaded software to networked storage devices without the approval of the Electronic Data Processing Department.

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 shall not be disabled, modified, uninstalled, or otherwise inactivated. If the user is uncertain as to whether the workstation the user is using is capable of detecting viruses automatically, or the user is unsure whether the data has been adequately checked for viruses, the user shall contact the Electronic Data Processing Department.

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

Encryption

Employees shall not assume electronic communications are private. Employees with a business-need to encrypt messages (e.g. for purposes of safeguarding sensitive or confidential information) shall submit a request to their Department Head. When authorized to use encryption by their supervisor and the Department Head, employees shall use encryption software supplied to them by the City. Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services who use encryption on files stored on a City computer must provide their Department Head with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys/codes necessary to access the files.

Participation in Online Forums

1. Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services 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.
2. The City 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 group devoted to the technical area.
3. Employees are encouraged to include the following disclaimer in all their posting 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 of Manitowoc."
4. Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services shall note that even with a disclaimer, a connection with the City exists, and a statement may be imputed legally to the City. Therefore, employees, officers, elected officials, boards, commissions, committees, contracted and consulting

services shall 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 city provided account. Communications shall not reveal confidential information and shall not otherwise violate this or other City policies.

Policy Violations

Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services who violate the Electronic Communications and Information Systems Policy may be subject to discipline, up to and including termination, and may be subject to civil liability and/or criminal prosecution.

SECTION 2 - E-MAIL POLICY

PURPOSE:

The City provides certain employees, officers, elected officials, boards, commissions, committees, contracted and consulting services 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 municipal 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. No expectation of privacy in regard to use of the City's e-mail system shall be expected by the employee, officers, elected officials, boards, commissions, committees, contracted and consulting services in any respect related to accessing, transmitting, sorting or communicating information via the system.

ORGANIZATIONS AFFECTED:

This policy applies to the entire City government including its departments, divisions, offices, officers, elected officials, boards, commissions, committees, City employees and contracted and consulting services (e.g. MPU I.T. department).

POLICY:

It is the policy of the City to follow this set of procedures for the use of the City's e-mail system of whatever kind and nature currently in existence and use, and hereafter placed in service by the City.

REFERENCES:

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

PROCEDURES:

Access to Employee E-mail

1. Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services shall 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 shall 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:
 - a. Access by the City's Electronic Data Processing Department during the course of system maintenance or administration;
 - b. Access approved by the employee, the employee's Department Head, or an officer of the City when there is an urgent business reason to access the employee's mailbox.
 - c. Access approved by the City Attorney and/or Human Resources Director and at least two of the following: the employee's Department Head, the Mayor or Council President when there is reason to believe the employee/official is using e-mail in violation of the City's policies;
 - d. Access approved by the City Attorney in response to the City's receipt of a court order or request from law enforcement and judicial officials for disclosure of an employee's e-mail messages.
2. Except as otherwise noted herein, e-mail should not be used to communicate sensitive or confidential information unless encrypted. Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services 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 shall be aware that a variety of human and system errors have the potential to cause inadvertent or accidental disclosures of e-mail messages.
 - a. The confidentiality of any message shall not be assumed. Even when a message is erased or deleted it is still possible to retrieve and read that message.

- b. Employees shall understand that electronic mail is a written form of communication, just like a paper letter, memo or other document. Though electronic mail is relatively spontaneous compared with regular mail, employees, officers, elected officials, boards, commissions, committees, contracted and consulting services should take care to use the same level of discretion and forethought before executing electronic messages.
3. All regular employees shall be issued a City e-mail address while employed at the City of Manitowoc. In addition, employees are required to monitor and read e-mails at least once a week. If an employee fails to receive information that was sent via e-mail due to not accessing the system regularly, the employee may be subject to disciplinary measures.

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.

1. Passwords are intended to keep unauthorized individuals from accessing messages stored on the system. 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.
2. The practice of using passwords shall 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 2, "Access to Employee E-mail").
3. Passwords shall never be given out over the phone, included in e-mail messages, posted, or kept within public view.
4. Employees are prohibited from disclosing their password, or those of any other employee, to anyone who is not an employee of the City; and then only on an "as needed" basis.

Employees also should not disclose their password to other employees, except when required by an urgent business matter (see Section 2 (1(b)) of this policy).

Personal Use

The City allows limited, occasional, or incidental personal use of its e-mail system during lunch, breaks or immediately before or after work, subject to the condition that personal use shall not:

- Involve any prohibited activity (see below);
- Interfere with the productivity of the employee or his or her co-workers;
- Involve large file transfers or otherwise deplete system resources available for business

purposes.

- Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services shall not have any expectations of privacy with respect to personal e-mail system. As e-mail is not private, employees shall avoid sending personal messages that are sensitive or confidential.

Prohibited Activities

1. Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services are strictly prohibited from sending e-mail or otherwise using the e-mail system in connection with any of the following activities:
 - Engaging in personal matters or entertainment on City time;
 - Engaging in illegal, fraudulent, or malicious activities;
 - 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);
 - Sending, viewing 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;
 - Annoying or harassing other individuals;
 - Using another individual's account or identity without explicit authorization;
 - Attempting to test, circumvent, or defeat security or auditing systems, without prior authorization;
 - Accessing, retrieving or reading any e-mail messages sent to other individuals, without prior authorization from the individual or Department Head (except persons authorized to access, retrieve or read any e-mail while investigating any possible violation of the policy).
 - Permitting any unauthorized individual to access the City's e-mail system.

Confidential Information

1. All employees, officers, elected officials, boards, commissions, committees, contracted and consulting services are expected to protect the City's confidential information. Employees, officers, elected officials, boards, commissions, committees, contracted and

consulting services shall not transmit or forward confidential information to others, except when there is a need to know, outside individuals or companies without the permission of their Department Head.

2. The City also requires its employees, officers, elected officials, boards, commissions, committees, contracted and consulting services to use e-mail in a way that respects the confidential and proprietary information of others. Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services are prohibited from copying or disturbing copyrighted material - for example, software, database files, documentation, or articles using the e-mail system.

Record Retention

The same rules which apply to record retention for other City paper and digital 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. If an email message needs to be retained longer than 180 days, it should be archived or saved outside of the email system itself.

The specific procedures to be followed with respect to the retention of e-mail are contained in Section 3, E-Mail Record Retention Policy.

E-mail Violation Policies

Employees violating the City's e-mail policy are subject to discipline, up to and including termination. Employees, officers, elected officials, boards, commissions, committees, contracted and consulting services using e-mail system for defamatory, illegal, or fraudulent purposes, and those who break into unauthorized areas of the City's computer system, also are subject to civil liability and criminal prosecution.

SECTION 3 - E-MAIL RECORD RETENTION POLICY

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 City documents apply to such records.

ORGANIZATIONS AFFECTED

This policy applies to all of the City of Manitowoc, including its departments, divisions, offices, officials, elected officials, boards, commissions, committees, employees and contracted and consulting services (e.g. MPU I.T. department).

POLICY

It is the policy of the City 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.

PROCEDURES:

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.

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.

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 shall be saved and shall be indexed so that it is linked to the related records in other media (for example, paper) so that a complete record can be assessed when needed. E-mail records to be retained shall be archived to an appropriate form of media. Any officer, elected official, commission, committee, board, department head, division head, or employee of the City may request assistance from the Legal Custodian of records in determining whether an e-mail is a public record. (The Clerk or the Clerk's designee is the keeper of the City records, Department Heads are the keeper of departmental records, the Chief of Police is Legal Custodian of Police Department records to name a few. See Section 19.33, Wis. Stats. which sets forth the legal custodian of a record.)

Responsibilities for E-mail Records

- Legal Custodian. E-mail records of a City authority having custody of records shall be maintained by the designated Legal Custodian, pursuant to City policy.
- Information Services. If e-mail is maintained in an on-line data base, it is the responsibility of the Information Technician to provide technical support for the Legal Custodian as needed. When equipment is updated, the Information Technician shall ensure that the ability to reproduce e-mail in a readable form is maintained. The

Information Technician shall assure that e-mail programs are properly set up to archive e-mail.

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 with the City Attorney, if necessary. As with other records, access to or electronic copies of disclosable records shall be provided within a reasonable time.

Violation

Employees violating this policy are subject to discipline up to and including dismissal. In addition employees, officers', elected officials', boards', commissions', committees', contracted and consulting services violations of this policy may be referred for civil and/or criminal prosecution, where appropriate.