

Electronic Communication & Information Systems Policy

I. Purpose. The purpose of this policy is to provide guidance on the proper use of the various electronic systems and services available to employees, including but not limited to computers, email, telephones, voicemail, on-line services, social media, cameras, laptops, and the Internet. This policy cannot provide rules to cover every possible situation. The purpose of the policy is to express the City's general philosophy and set forth guidelines governing the use of electronic systems and services. Employees who abuse this policy risk having privileges or resources removed from them, and could be subject to discipline up to and including discharge, civil liability, and criminal prosecutions.

II. Organizations Affected. This policy applies to the City of Manitowoc, including departments, offices, boards, commissions, committees, and employees.

III. Access and Authority. Department Heads shall determine access to systems and services, and who shall have authority to communicate on behalf of the City. The provisions of this policy shall apply to the use of City-owned and provided equipment, regardless of the location of usage.

IV. Privacy. Electronic information created and/or communicated by an employee using City email, utility programs, voice mail, telephones, internet systems, faxes, computer documents, and similar electronic media may be accessed and monitored by the City. The City reserves the right to review, monitor, intercept, access, and disclose all messages created, received, or sent over electronic communication systems.

V. Prohibited Usage.

- a. Electronic systems and services cannot be used for knowingly transmitting, retrieving, or storing any communications that include, but are not limited to:
 - i. Personal business on City time, except as otherwise permitted by this Policy
 - ii. Discriminatory or harassing
 - iii. Derogatory to any individual or group
 - iv. Obscene, as defined in Wis. Stat. § 944.21
 - v. Defamatory, threatening, fraudulent, or malicious
 - vi. Illegal
 - vii. Contrary to any City policy or the best interests of the City
 - viii. Sent with intent to frighten, intimidate, threaten, abuse or harass
 - ix. Materials considered offensive, including but not limited to: those with sexual implications, nude images, racial slurs, gender-specific comments, or any other comment offensively addressing someone's age, race, creed, color, sex, ancestry, religious or political beliefs, marital status, sexual orientation, national origin, or disability
 - x. Using another individual's account or identity without explicit authorization
 - xi. An attempt to test, circumvent, or defeat security or auditing systems, without prior authorization
 - xii. An attempt to access, retrieve, or read any email message or attachments sent to another individual, unless authorized
 - xiii. Sending City-wide group emails for non-work related issues
 - xiv. Permitting any unauthorized individual to access the City's system

- b. Employees should not download or transfer software onto the City system without the approval of the IT Department.
- c. Employees should not use software without appropriate licenses.
- d. Printers, copiers, and fax machines are provided strictly for City business purposes. Any personal usage should be minimal and approved by a supervisor.
- e. Employee owned devices should not be connected to the City network without supervisor approval.
- f. Freeware or shareware is not authorized on City devices unless endorsed by the IT department, who will verify license usage.

VI. Authorized Personal Use of Computers or iPads. Electronic systems and services are provided for business usage during City time. Limited, occasional, or incidental use of electronic systems for personal, non-business purposes is permitted as set forth below unless restricted elsewhere:

- a. Personal usage is allowed during breaks, lunch, or immediately before/after work
- b. Personal use must not interfere with productivity of the employee or coworkers
- c. Personal use may not involve any prohibited activity
- d. Personal use must not consume system resources or storage capacity on an ongoing basis
- e. Personal use must not deplete system resources for business purposes
- f. Employees shall have no expectation of privacy when using the City's electronic systems and services for personal usage.

VII. Telephone and Cell Phone Usage. City phones and cellular phones are to be used for City business. Brief, limited, personal use is permitted during the day.

VIII. Security. Employees must respect the confidentiality of other individuals' electronic communications. Employees should not divulge their passwords and are expected to comply with all IT policies regarding passwords and login credentials.

IX. Email Special Emphasis. The purpose of this section is to emphasize that most emails sent using the City email system are public records. The same rules which apply to record retention and disclosure for other City documents apply to email as well.

- a. **Nature of Email.** As a general rule, emails sent on the City system are considered a public record whenever a paper message (letter or memo) having the same content would be a public record. See Wis. Stat. § 19.32(2) for the definition of a record. This includes the message, the identities of the sender and all recipients, the date, and any non-archived attachments to the email, as well as return receipts.
- b. **Public Access to Email Records.** If a department receives a request for release of an email, they should contact the City Attorney's office for advice prior to release.
- c. **Access to Email Records by Anyone Other than the Account User.** While the City reserves the right to access employee emails at any time, information contained in the email system shall only be disclosed to the extent permitted by law, for business purposes, or as needed to enforce City policies. When email is accessed by someone other than the account holder, it should be done for one of the following reasons:
 - i. Access by the IT department for system maintenance or administration
 - ii. Access approved by the employee, the Employee's Department Head, or an officer of the City, when done for an urgent business reason.
 - iii. Access approved by the City Attorney or the Human Resources Director and at least one of the following: the Mayor, the Council President, and the

Employee's Department Head when there is reason to believe the employee is using email in violation of City policies.

iv. Access by the City Attorney or designated staff to comply with a court order, open records request, or request from law enforcement.

d. Regular Use of Email. All employees are issued a City email address and are expected to monitor and read emails at least once a week. If an employee fails to receive information sent via email due to failure to check their email, they may be subject to discipline.

e. Personal Use of Email. Personal use of the email system should be avoided.

X. Out of Office. Employees are expected to set their out of office messages on their voicemail and email systems if they will be out of the office for 8 hours or more.