



CITY OF GREEN BAY PERSONNEL POLICY

Policy Title Electronic Communication and Information Systems Usage	Policy Reference Chapter 19
Policy Source Human Resources Department	Legal Review Date
Personnel Committee Approval	City Council Approval Updated March 3, 2015

- 19.1 **Purpose.** The purpose of this policy is to provide guidance on the proper use of the various electronic systems available to employees. Electronic systems include computers, e-mail, telephones, cellular telephones, pagers, voice mail, facsimiles, external electronic bulletin boards, wire services, on-line services, cameras, laptops, PDA's, and the Internet. This policy cannot provide rules to cover every possible situation. The purpose of this policy is to express the City's philosophy and set forth general guidelines governing the use of electronic systems and services. Employees who abuse this policy risk having the privilege removed for them and possibly other employees are subject to discipline, up to and including discharge and may be subject to civil liability and criminal prosecution.
- 19.2 **Organizations Affected.** This policy applies to all of the City of Green Bay government, including its Departments, Offices, Boards, Commissions, Committees, employees and contracted/consulting resources.
- 19.3 **Access and Authority.**
- 19.3.1 Each Department Head shall determine which employees in their department shall have access to the various systems and services, based on business practices and necessity and which shall have authority to communicate on behalf of the City.
- 19.3.2 The provisions of this Policy shall apply to the use of City-owned and 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.
- 19.4 **Privacy.** Electronic information created and/or communicated by an employee using e-mail, utility programs, voice mail, City telephones, City cell phones, internet and bulletin board systems, desktop faxes, all computer documents, and similar electronic media may be accessed and monitored by the City. The City 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 as required.

19.5 Prohibited System Usage.

19.5.1 Electronic systems and services cannot be used for knowingly transmitting, retrieving or storing any communication that include but are not limited to:

- a. Personal business on City time (e.g. sports pools, games, shopping, correspondence or other non-business-related items/documents), except as otherwise allowed under 19.6,
- b. Discriminatory or harassing,
- c. Derogatory to any individual or group,
- d. Obscene as defined in Wis. Stats. § 944.21,
- e. Defamatory, threatening, fraudulent, or malicious,
- f. Illegal or contrary to the City's policy or business interests,
- g. Engaging in the unlawful use of the e-mail system as set forth in Wis. Stats. § 947.0125 (unlawful use of computerized communication systems),
- h. Materials which are considered offensive include, but are not limited to: any materials which contain sexual implications, nude images, 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,
- i. Using another individual's account or identity without explicit authorization,
- j. An attempt to test, circumvent, or defeat security or auditing systems, without prior authorization,
- k. An attempt to access, retrieve or read any e-mail message sent to other individuals, unless authorized,
- l. Sending city-wide group emails on non-work related issues or for events not sponsored by the city,
- m. Permitting any unauthorized individual to access the City's e-mail system.

19.5.2 For the protection, integrity and security of the City's network, electronic systems shall not be used to download or transfer software, unless authorized by the IT Division. Do not copy software for use on another City PC, for personal use, or for distribution to others unless a legal license is procured.

19.5.3 Printers, copiers, and facsimiles are provided strictly for City business purposes. The City must be reimbursed for personal use of these machines at a rate of \$.25 per page payable to the City Clerk's Office.

19.5.4 Employee owned devices, such as personal data assistants (PDA's), digital cameras, printers, network access points, digital media readers, audio speakers, portable digital storage devices, voice answering machines, laptops, keyboards, and mice should not be connected to City computers or networks unless

authorization is received by the IT Division.

19.5.5 Freeware and shareware is not permitted on City computers unless provided or endorsed by the IT Division. Unauthorized use or independent installation of non-standard software or data may cause computers and networks to function erratically, improperly, or cause data loss. Personal licensed software is not permitted due to the liability the City is placed in if the licensing requirements are violated.

19.6 Authorized Personal Use. Except as otherwise provided, electronic systems and services provided by the City are for employees' business use during City time. Limited, occasional, or incidental use of electronic systems (sending or receiving) for personal non-business purposes is permitted as set forth below unless restricted elsewhere:

19.6.1 Personal use is allowed during breaks, lunch or immediately before/after work.

19.6.2 Personal use must not interfere with the productivity of the employee or co-workers.

19.6.3 Personal use does not involve any prohibited activity.

19.6.4 Personal use does not consume system resources or storage capacity on an ongoing basis.

19.6.5 Personal use does not involve large file transfers or otherwise deplete system resources available for business purposes.

19.6.6 Any cost associated with personal use of City resources must be reimbursed to the City.

19.7 Telephone And Cell Phone Usage

19.7.1 City telephones and cellular phones are to be used for City business. However, brief, limited personal use (5 minutes or less per day) is permitted during the workday. Personal long distance calls are only permitted with the use of a personal 1-800 calling card.

19.7.2 The use of personal cell phones for personal calls should be limited to 5 minutes or less per day.

19.7.3 The use of cell phones, except for hands-free activations, is prohibited while driving a City vehicle, with the exception of emergency vehicles, under emergency conditions.

19.8 Security. Employees must respect the confidentiality of other individuals' electronic communications. Employees are prohibited from engaging in or attempting to engage in:

- a. Monitoring or intercepting the files or electronic communications of other employees or third parties.
- b. Hacking or obtaining access to systems or accounts they are not authorized to use.
- c. Disabling, modifying, uninstalling, or otherwise inactivating virus scanning

software.

- d. Using other people's logins or passwords unless authorized.
- e. Breaching, testing, or monitoring computer or network security measures.

19.8.1 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.

19.8.2 Anyone obtaining electronic access to other organizations, businesses, 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.

19.8.3 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.

19.8.4 Passwords are intended to keep unauthorized individuals from accessing messages stored on the system. Passwords also establish the identity of the person sending an e-mail message.

- a. Passwords should never be given out over the phone, included in e-mail messages, posted, or kept within public view.
- b. Users should logout or lock their computer with the password protected screen saver if their computer is in a non-secure area. Users should logout of their computer at the end of their workday.
- c. Employees are prohibited from disclosing their password to anyone who is not an employee of the City. Employees also should not disclose their password to other employees, except when authorized.

19.9 E-Mail Special Emphasis. The purpose of this section 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 of Green Bay documents, apply to such records.

19.9.1 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.

19.9.2 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 sender received the message is also considered to be part of the record.

19.9.3 Public Access to E-Mail Records. If a Department receives a request for release of an e-mail the Law Department should be contacted to determine if it is appropriate for public release. The Law Department and/or HR will review the email(s) and determine whether to release them to the public.