ELECTRONIC COMMUNICATION & INFORMATION SYSTEMS POLICY

I. ELECTRONIC COMMUNICATION

A. PURPOSE

To better serve our citizens and give our workforce the best tools to do their jobs, the Common Council of the City of Middleton (the City) 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, social networks, the Internet, text messaging, and the World Wide Web.

The City 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 anticipated 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'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. Where the policy notes "unless authorized by the City Administrator", it should be understood that the City Administrator will delegate such authority in most instances to the Information Services Director; consequently, requests should be sent to both individuals for consideration.

1. The following procedures apply to all electronic media and services used by City officers or employees that are:
    a. Accessed on or from City premises on City work time;
    b. Used in a manner that expressly or implicitly states that the individual as acting for or on behalf of the City.
    c. Provided or owned by the City.

2. Organizations affected
    This policy applies to all of the City of Middleton's departments, offices, boards, commissions, committees, City employees and contracted and consulting resources.

B. POLICY

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

1. 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 City.
   b. The provisions of this Policy shall apply to the use of City-owned/provided equipment from home or other locations off City premises. City-owned equipment (e.g. lap tops, cell phones, etc.) 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. Obscene as defined in Wis. Stats. § 944.21;
      iv. Defamatory or threatening; or
      v. 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 electronic communications systems, electronic media shall not be used to download or transfer software, unless authorized by the City Administrator. No one covered by this policy shall take, alter, forge, copy, tamper with, disseminate or delete any kind of City electronic media or record without proper authorization.

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. Brief, limited personal use is permitted during the work day; however, personal use should be limited largely to breaks, lunch or immediately before/after work;
      ii. Personal use must not interfere with the productivity of the employee or that of his or her co-workers;
      iii. Personal use does not involve any prohibited activity (see Section I.C.2);
      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 during the employee's standard work day. However, brief, limited personal use is permitted during the work day. Personal long distance calls are only permitted within the limits of the City's phone service plan. Calls made outside the limits of the City's plan shall be reimbursed to the City.
   c. Employees shall 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 or communicated by an employee using e-mail, word processing, utility programs, spreadsheets, voice mail, telephones, internet and bulletin board systems, desktop faxes, text messaging, 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 its 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 be performed in compliance with federal and state law.

5 Security/Appropriate Use

a. Except in cases in which explicit authorization has been granted under the authority of the City Administrator, employees are prohibited from engaging in, or attempting to engage in (except for law enforcement pursuant to a court order, search warrant, search warrant exception, exception to the Wisconsin Electronic Surveillance Control Law, or as otherwise permitted by law for official police investigations):
   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 shall be sent that attempt to hide the identity of the sender or represent the sender as someone else.

c. Electronic media and services shall 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 materials belonging to other organizations, businesses, companies, municipalities or individuals must respect all copyrights and shall not copy, retrieve, modify, or forward copyrighted materials except as permitted by the copyright owner.

e. 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 Services Department. Users must never install downloaded software to networked storage devices without the assistance and approval of appropriate personnel.

f. 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 shall not be disabled, modified, uninstalled, or otherwise inactivated. When uncertain as to whether a workstation is capable of detecting viruses automatically, or whether the data has been adequately checked for viruses, the user shall contact the Information Services Department.

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

6. Encryption

Employees shall 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 the City Administrator's office. When authorized to use encryption by their supervisor and the City Administrator's office, employees shall use encryption software supplied to them by the Information Services Department. Employees who use encryption on files stored on a City 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. 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.

b. 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 newsgroup devoted to the technical area.

c. A connection with the City exists with respect to all communications transmitted with City provided equipment or facilities and any such statements could be imputed legally to the City. Instead, employees should seek to limit their discussion to matters of fact and avoid expressing opinions while using the City's systems or City provided account unless such expression is necessary to fulfill the legitimate objectives of the communication. Communications shall not reveal confidential information or otherwise violate this or other City policies.

d. Employees must receive authorization from their Department Heads prior to participating in an on-line forum on City equipment or on standard City work time. 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 and 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 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 use of City equipment or during the employee's work hours, 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 regards to use of the City's e-mail system exists 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, and City employees. It also applies to emails sent to or received from contracted and consulting resources.

B. POLICY

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

1. 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 City Administrator's Office during the course of system maintenance or administration;
      ii. Access approved by the employee, the employee's supervisor, the City Administrator's office or the City Attorney 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 City Administrator's office or the City Attorney 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's office 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 or as authorized by a department head and City Administrator, 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 shall 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 City Administrator's office.

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 is not cause for 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 shall not 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 II C. 1. a. ii. of this policy).

3. Personal Use

a. 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 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 shall have no expectation 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. Employees should not erase or delete any emails where City business or City affairs are referenced. However, the aforementioned deletion prohibition does not apply to auto archiving.

Personal use on City equipment and the history and logs of that use, residual email trails, and not fully erased or deleted emails that remain on City equipment after use are the City's property and are subject to disclosure to City staff and officials and may be subject to public disclosure pursuant to Wisconsin's Public Records Law. If personal e-mails on a City electronic communications system are determined to be public records they shall not be deleted except upon expiration of the applicable retention period. For such electronic records as public records, the City typically must retain such documents for as seven (7) years.

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 City time except as permitted under Section 3 above;
        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, , 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 City Administrator's office; 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'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's office. 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 procedures to be followed with respect to the retention of e-mail records is contained in Section III, E-Mail Record Retention Policy.

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 Administrator's office. Employees with a business need to encrypt messages should submit a written request to their supervisor and the City Administrator's office. When authorized to use encryption by their supervisor and the City Administrator's office, employees shall use encryption software supplied to them by the City Administrator's office. 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'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 City documents apply to such records.

1. Organizations affected:
   This policy applies to all of the City of Middleton's divisions, offices, boards, commissions, committees, employees and contracted and consulting resources.

B. POLICY

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

1. 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 archivable 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 Legal Custodian of records (the City Clerk or the Clerk's designee, except that the Chief of Police is Legal Custodian of Police Department records) 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 authority having custody of records shall be maintained by the designated Legal Custodian, pursuant to City policy.
   b. Information Services Manager. If e-mail is maintained in an on-line data base, it is the responsibility of the City's network service provider to provide technical support for the Legal Custodian as needed. When equipment is updated, the City Administrator's office shall ensure that the ability to reproduce e-mail in a readable form is maintained. The City Administrator's office 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, if necessary. As with other records, access to or electronic copies of disclosable records shall be provided as soon as practicable and without delay.

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 or criminal prosecution, where appropriate.

E-MAIL AND ELECTRONIC COMMUNICATIONS POLICIES

EMPLOYEE NOTICE

As an employee of the City of Middleton (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 City Administrator's office.

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, and have been afforded an opportunity to ask questions regarding the policy. I also acknowledge that I have read and that I understand this notice.

_____ _____

Signature of Employee Date

_____ _____

Signature of Supervisor Date

Copy for Employee

E-MAIL AND ELECTRONIC COMMUNICATIONS POLICIES

EMPLOYEE NOTICE

As an employee of the City of Middleton (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 City Administrator's office.

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, and have been afforded an opportunity to ask questions regarding the policy. I also acknowledge that I have read and that I understand this notice.

_____ _____

Signature of Employee Date

_____ _____

Signature of Supervisor Date

Copy for Employee's Personnel File

4846-8336-1799, v. 1