

**CITY OF STOUGHTON**  
**ELECTRONIC COMMUNICATION & INFORMATION SYSTEMS POLICY**

Council adopted 11/9/04

**SECTION 1 - ELECTRONIC COMMUNICATION**

1.1 **PURPOSE:**

To better serve our citizens and give our workforce the best tools to do their jobs, the Governing Unit of City of Stoughton (the "Governing Unit") 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, the Internet, and the World Wide Web.

The Governing Unit 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 Governing Unit should remember that electronic media and services provided by the Governing Unit are Governing Unit property and their purpose is to facilitate and support Governing Unit business. No expectation of privacy in regards to use of the Governing Unit's electronic communication systems should be expected 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 Governing Unit's philosophy and set forth general guidelines governing the use of electronic media and services. By adopting this policy, it is the Governing Unit'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 Governing Unit.

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

Accessed on or from Governing Unit premises;

Accessed using Governing Unit computer equipment or via Governing Unit-paid access methods; or

Used in a manner that identifies the individual as acting for or on behalf of the Governing Unit; or in anyway identifies the Governing Unit.

1.2 **ORGANIZATIONS AFFECTED:**

This policy applies to all of the Governing Unit of City of Stoughton, including its departments, offices, boards, commissions, committees, Governing Unit employees and contracted and consulting resources.

1.3 **POLICY:**

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

1.4 **REFERENCES:**

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

1.5 PROCEDURES:

1.5. A 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 Governing Unit.
- 2) The provisions of this Policy shall apply to the use of Governing Unit-owned/provided equipment and/or services from home or other locations off Governing Unit premises. Governing Unit-owned equipment (e.g. lap tops) may be removed from Governing Unit premises solely for Governing Unit work related purposes pursuant to prior authorization from the Department Head.

1.5. B PROHIBITED COMMUNICATIONS

- 1) Electronic media cannot be used for knowingly transmitting, retrieving or storing any communication that is:
  - a) Personal business on Governing Unit time (e.g. sports pools, games, shopping, correspondence or other non-business-related items/documents), except as otherwise allowed under Section 1.5.C;
  - b) Discriminatory or harassing;
  - c) Derogatory to any individual or group;
  - d) Obscene as defined in Wis. Stats. § 944.21;
  - e) Defamatory or threatening; or
  - f) Engaged in for any purpose that is illegal or contrary to the Governing Unit's policy or business interests.
- 2) For the protection, integrity and security of the Governing Unit's System, electronic media shall not be used to download or transfer software, unless authorized by the Director of Planning & Development.

1.5. C PERSONAL USE

- 1) Except as otherwise provided, electronic media and services are provided by the Governing Unit for employees' business use during Governing Unit time. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal non-business 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 1.5.B, b-f);
  - d) Personal use does not consume system resources or storage capacity on an ongoing basis;
  - e) Personal use does not involve large file transfers or otherwise deplete system resources available for business purposes.
- 2) Governing Unit telephones and cellular phones are to be used for Governing Unit business. However, brief, limited personal use is permitted during the work day. Personal long distance calls are only permitted with the use of a personal 1-800 calling card, or with the understanding that such calls must be reimbursed to the Governing Unit.
  - 3) Employees should not have any expectation of privacy with respect to personal use of the Governing Unit's electronic media or services.

#### 1.5. D ACCESS TO EMPLOYEE COMMUNICATIONS

- 1) Electronic information created and/or communicated by an employee using e-mail, word processing, utility programs, spreadsheets, voice mail, telephones, Internet and bulletin board systems, desktop faxes, and similar electronic media may be accessed and monitored by the Governing Unit. The Governing Unit respects its employees' desire to work without surveillance. However, the Governing Unit 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 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 Governing Unit 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.

#### 1.5. E SECURITY/APPROPRIATE USE

- 1) Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by the Department Head, 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) Using other people's log-ins or passwords; 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 should 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.
  - 4) Anyone obtaining electronic access to other organizations', business', 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.

Employees 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 the assistance of the Director of Planning & Development, except Stoughton Municipal Utilities employees shall contact the Utilities Consumer Services/Information Systems Technician. Users must never install downloaded software to networked storage devices without the assistance and approval of appropriate personnel.

Most of the Governing Unit'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 must not be disabled, modified, uninstalled, or otherwise inactivated. If you are uncertain as to whether the workstation you are using is capable of detecting viruses automatically, or you are unsure whether the data has been adequately checked for viruses, you should contact the Director of Planning & Development, except Stoughton Municipal Utilities employees shall contact the Utilities Consumer Services/Information Systems Technician.

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.

#### 1.5. F ENCRYPTION

Employees should 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 Department Head. When authorized to use encryption by their supervisor and the Department Head, employees shall use

encryption software supplied to them by the Director of Planning & Development, except Stoughton Municipal Utilities employees shall contact the Utilities Consumer Services/Information Systems Technician. Employees who use encryption on files stored on a Governing Unit 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.

#### 1.5. G PARTICIPATION IN ON-LINE FORUMS

- 1) Employees should remember that any messages or information sent on Governing Unit-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 Governing Unit.
- 2) The Governing Unit 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.
- 3) Employees shall include the following disclaimer in all of their postings 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 Governing Unit of the City of Stoughton."
- 4) Employees should note that even with a disclaimer, a connection with the Governing Unit exists and a statement could be imputed legally to the Governing Unit. Therefore, employees should not rely on disclaimers as a way of insulating the Governing Unit 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 Governing Unit's systems or Governing Unit provided account. Communications must not reveal confidential information and must not otherwise violate this or other Governing Unit policies.
- 5) Employees must receive authorization from their Department Heads prior to participating in an on-line forum. The employees shall be required to review the provisions of this section before they receive such authorization.

#### 1.5. H POLICY VIOLATIONS

Employees who abuse the privilege of Governing Unit-facilitated access to electronic media or services risk having the privilege removed for themselves and possibly other employees, are subject to discipline, up to and including termination and may be subject to civil liability and criminal prosecution.

### **SECTION 2 - E-MAIL POLICY**

#### 2.1 PURPOSE:

The Governing Unit 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 Governing Unit building, or thousands of miles away.

The Governing Unit'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 Governing Unit and may constitute public records. This policy explains rules governing the appropriate use of e-mail and sets out the Governing Unit's rights to access messages on the e-mail system. No expectation of privacy in regards to use of the Governing Unit's e-mail system should be expected by the employee in any respect related to accessing, transmitting, sorting or communicating information via the system.

2.2 ORGANIZATIONS AFFECTED:

This policy applies to all Governing Unit departments, divisions, offices, boards, commissions, committees, Governing Unit employees and contracted and consulting resources.

2.3 POLICY:

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

2.4 REFERENCES:

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

2.5 PROCEDURES:

2.5. A ACCESS TO EMPLOYEE E-MAIL

1) Employees should not have any expectation of privacy with respect to messages or files sent, received, or stored on the Governing Unit's e-mail system. E-mail messages and files, like other types of correspondence and Governing Unit documents, can be accessed and read by authorized employees or authorized individuals outside the Governing Unit. The Governing Unit 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:

- a) Access by the Director of Planning & Development during the course of system maintenance or administration;
- b) Access approved by the employee, the employee's supervisor, or an officer of the Governing Unit 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;

- c) Access approved by the employee's supervisor, the Director of Planning & Development, or an officer of the Governing Unit when there is reason to believe the employee is using e-mail in violation of the Governing Unit's policies;
  - d) Access approved by the Director of Planning & Development or the Governing Unit Attorney in response to the Governing Unit's receipt of a court order or request from law enforcement 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. 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 Governing Unit 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.
  - 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.
  - 4) 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.

#### 2.5. B 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 and Director of Planning & Development, except Stoughton Municipal Utilities employees, shall contact the Utilities Consumer Services/Information Systems Technician.

- 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.
- 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 2.5.A, "Access to Employee E-mail").
- 3) Passwords should 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 Governing Unit. Employees also should not disclose their password to other employees, except when required by an urgent business matter (see Section 2.5.A.1(b) of this policy).

#### 2.5. C PERSONAL USE

- 1) The Governing Unit 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:
  - a) Personal use must not:
    - i) Involve any prohibited activity (see Section 2.5.D);
    - 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.
  - b) Employees should not have any expectations of privacy with respect to personal e-mail sent or received on the Governing Unit'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.

#### 2.5. D PROHIBITED ACTIVITIES

- 1) Employees are strictly prohibited from sending e-mail or otherwise using the e-mail system in connection with any of the following activities:
  - a) Engaging in personal business or entertainment on Governing Unit time;
  - b) Engaging in illegal, fraudulent, or malicious activities;
  - c) 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);
  - d) 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;

- e) Annoying or harassing other individuals;
- f) Using another individual's account or identity without explicit authorization;
- g) Attempting to test, circumvent, or defeat security or auditing systems, without prior authorization;
- h) Accessing, retrieving or reading any e-mail messages sent to other individuals, without prior authorization from the Department Head; or
- i) Permitting any unauthorized individual to access the Governing Unit's e-mail system.

#### 2.5. E CONFIDENTIAL INFORMATION

- 1) All employees are expected and required to protect the Governing Unit's confidential information. Employees shall not transmit or forward confidential information to outside individuals or companies without the permission of their supervisor and the Department Head. See Section 2.5.G, Encryption.
- 2) The Governing Unit 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.

#### 2.5. F RECORD RETENTION

- 1) The same rules which apply to record retention for other Governing Unit 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.
- 2) The specific procedures to be followed with respect to the retention of e-mail records is contained in Section 3, E-Mail Record Retention Policy.

#### 2.5. G ENCRYPTION

Encrypting e-mail messages or attached files sent, stored, or received on the Governing Unit'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 Department Head. Employees with a business need to encrypt messages should submit a written request to their supervisor and the Department Head. When authorized to use encryption by their supervisor and the Department Head, employees shall use encryption software supplied to them by the Director of Planning & Development, except Stoughton Municipal Utilities employees shall contact the Utilities Consumer Services/Information Systems Technician. Employees who use encryption on e-mail stored on a Governing

Unit 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.

#### 2.5. H E-MAIL POLICY VIOLATIONS

Employees violating the Governing Unit'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 Governing Unit's computer system also are subject to civil liability and criminal prosecution.

### **SECTION 3 - E-MAIL RECORD RETENTION POLICY**

#### 3.1 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 Governing Unit documents apply to such records.

#### 3.2 ORGANIZATIONS AFFECTED:

This policy applies to all of the Governing Unit of City of Stoughton, including its departments, divisions, offices, boards, commissions, committees, Governing Unit employees and contracted and consulting resources.

#### 3.3 POLICY:

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

#### 3.4 REFERENCES:

Wis. Stats. §§16.612, 19.21 et. seq., 19.32 and 19.33.

#### 3.5 PROCEDURES:

##### 3.5. A 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.

##### 3.5. B 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.

##### 3.5. C SAVING AND INDEXING E-MAIL RECORDS

Initially the custodian (that officer, department head, division head, or employee of the Governing Unit 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 Governing Unit may request assistance from the Legal Custodian of records (the Governing Unit 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.

#### 3.5. D RESPONSIBILITIES FOR E-MAIL RECORDS MANAGEMENT

- 1) Legal Custodian. E-mail records of a Governing Unit authority having custody of records shall be maintained by the City Clerk.
- 2) Information Services Manager. If e-mail is maintained in an on-line data base, it is the responsibility of the Director of Planning & Development, except Stoughton Municipal Utilities employees shall contact the Utilities Consumer Services/Information Systems Technician to provide technical support for the Legal Custodian as needed. When equipment is updated, the Director of Planning & Development, except Stoughton Municipal Utilities employees shall contact the Utilities Consumer Services/Information Systems Technician shall ensure that the ability to reproduce e-mail in a readable form is maintained. The Director of Planning & Development, except Stoughton Municipal Utilities employees shall contact the Utilities Consumer Services/Information Systems Technician shall assure that e-mail programs are properly set up to archive e-mail as required by the City Clerk.

#### 3.5. E 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 Governing Unit Attorney, if necessary. As with other records, access to or electronic copies of disclosable records shall be provided within a reasonable time.

#### 3.5. F 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 and/or criminal prosecution, where appropriate.

Approved by the Common Council 11-9-04

**E-MAIL AND ELECTRONIC COMMUNICATIONS POLICIES**

**EMPLOYEE NOTICE**

As an employee of the Governing Unit of City of Stoughton (the "Governing Unit"), I recognize and understand that the Governing Unit's electronic communication systems are provided for conducting the Governing Unit's business. However, Governing Unit 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 Governing Unit. I agree not to use the electronic communication systems in a way that is disruptive, offensive, or harmful to others or to the Governing Unit. 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 Department Head.

I am aware that the Governing Unit reserves and will exercise the right to review, audit, intercept, access and disclose all matters on the Governing Unit's electronic communications systems at any time. I am aware that the Governing Unit 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 Governing Unit'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 Governing Unit'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 Governing Unit of City of Stoughton (the "Governing Unit"), I recognize and understand that the Governing Unit's electronic communication systems are provided for conducting the Governing Unit's business. However, Governing Unit 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 Governing Unit. I agree not to use the electronic communication systems in a way that is disruptive, offensive, or harmful to others or to the Governing Unit. 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 Department Head.

I am aware that the Governing Unit reserves and will exercise the right to review, audit, intercept, access and disclose all matters on the Governing Unit's electronic communications systems at any time. I am aware that the Governing Unit 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 Governing Unit'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 Governing Unit'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*