

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

*adopted by the Common Council of the City of Stoughton 11/09/2004;  
revised to add social networking policy and adopted 09/10/2013*

**SECTION 1: ELECTRONIC COMMUNICATIONS**

**1.1 PURPOSE**

To better serve our citizens and give our workforce the best tools to do their jobs, the City of Stoughton (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, the Internet, 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. There should be no expectation of privacy for any employee in any respect related to accessing, transmitting, sorting, or communicating information via the City's electronic communication 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.

The following procedures apply to all electronic media and services that are accessed on or from City premises; accessed using City computer equipment or via City-paid access methods; or used in a manner that identifies the individual as acting for or on behalf of the City; or in any way identifies the City.

**1.2 ORGANIZATIONS AFFECTED**

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

**1.3 POLICY**

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

**1.4 AUTHORITY**

Electronic communications and information technology are overseen for the City of Stoughton by the Director of Planning & Development. Stoughton Utilities has its own system, which is overseen by the Utilities Office and Information Systems Supervisor. In all cases where any question shall arise, Stoughton Utilities employees should contact the Utilities Office and Information Systems Supervisor; all other employees should contact the Director of Planning & Development.

**1.5 REFERENCES**

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

## 1.6 PERSONAL USE

1.6. A. Except as otherwise provided, electronic media and services, including e-mail, 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. Personal use is limited to breaks, lunch or immediately before/after work;
- ii. Personal use must not interfere with the productivity of the employee or his/her co-workers;
- iii. Personal use does not involve any prohibited activity (see Section 1.6.A-J);
- 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.

1.6. B. 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 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 City.

1.6. C. Employees should not have any expectation of privacy with respect to personal use of the City's electronic media or services, or 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.

## 1.7 PROHIBITED ACTIVITIES/COMMUNICATIONS

Employees may not use the City's e-mail system or other electronic media for:

1.7. A. Personal business or entertainment on City time (e.g. sports pools, games, shopping, correspondence or other non-business-related items/documents), except as otherwise allowed under Section 1.5.A;

1.7. B. Engaging in illegal, fraudulent, or malicious activities;

1.7. C. Engaging in activities that are contrary to the City's policies or business interests;

1.7. D. 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);

1.7. E. Knowingly transmitting, retrieving, or storing offensive, disruptive, obscene (as defined in Wis. Stats. § 944.21), defamatory, or threatening 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;

1.7. F. Annoying or harassing other individuals;

- 1.7. G. Using another individual's account or identity without explicit authorization;
- 1.7. H. Attempting to test, circumvent, or defeat security or auditing systems, without prior authorization;
- 1.7. I. Accessing, retrieving or reading any e-mail messages sent to other individuals, without prior authorization from the Department Head; or
- 1.7. J. Permitting any unauthorized individual to access the City's e-mail system or social media accounts.

For the protection, integrity and security of the City's system, electronic media shall not be used to download or transfer software, unless authorized by the Director of Planning & Development.

#### 1.8 ACCESS TO EMPLOYEE COMMUNICATIONS

1.8. A. 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 City. The City respects its employees' desire to work without surveillance. However, 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 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.

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

#### 1.9 SECURITY/APPROPRIATE USE

1.9. A. 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:

- 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.

1.9. B. 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.

1.9. C. 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.

1.9. D. 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.

1.9. E. 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. Stoughton Utilities employees shall contact the Utilities Office and Information Systems Supervisor. Users must never install downloaded software to networked storage devices without the assistance and approval of appropriate personnel.

1.9. F. 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. Stoughton Utilities employees shall contact the Utilities Office and Information Systems Supervisor.

1.9. G. 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.

#### 1.10. ENCRYPTION

1.10. A. 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. Stoughton Utilities employees shall contact the Utilities Office and Information Systems Supervisor.

1.10. B. 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.

#### 1.11. POLICY VIOLATIONS

Failure to comply with this policy may result in disciplinary action. Disciplinary action may involve a verbal or written warning or, in serious cases, termination of employment.

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; are subject to discipline, up to and including termination; and may be subject to civil liability and criminal prosecution.

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

The City provides its employees with the capability to send and receive electronic mail (e-mail) so they can work more productively. The messages sent and received on the e-mail system, like memos, purchase orders, letters, and other documents created by employees in the course of their workday, are the property of the City and may constitute public records. This section of the electronic communications 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.

#### 2.1 ACCESS TO EMPLOYEE E-MAIL

2.1. A. Authorized access to employee e-mail by other employees or outside individuals includes, but is not limited to, the following:

- i. Access by the Director of Planning & Development during the course of system

maintenance or administration;

ii. Access approved by the employee, the employee's supervisor, or an officer of the City 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 Director of Planning & Development, or an officer of the City when there is reason to believe the employee is using e-mail in violation of the City's policies;

iv. Access approved by the Director of Planning & Development 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.

2.1. B. Except as otherwise noted herein, e-mail should not be used to communicate sensitive or confidential information. The confidentiality of any message should not be assumed. E-mail can easily be forwarded to third parties. Even when a message is erased, it is still possible to retrieve and read that message.

## 2.2. 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 Department Head and Director of Planning & Development or the Stoughton Utilities Office and Information Systems Supervisor.

2.2. A. 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.

2.2. B. 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 2.1, "Access to Employee E-mail").

2.2. C. Passwords should never be given out over the phone, included in e-mail messages, posted, or kept within public view.

2.2. 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 2.1.A.ii of this policy).

## 2.3. CONFIDENTIAL INFORMATION

2.3. 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 Department Head. See Section 1.10, Encryption.

2.3. 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.

## 2.4. RECORD RETENTION

2.4. 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.

2.4. B. 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. ENCRYPTION

2.5. A. 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 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 or the Stoughton Utilities Office and Information Systems Supervisor.

2.5. B. 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.

## 2.6. 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.

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

### 3.1 PURPOSE:

The purpose of this section of the City of Stoughton's Electronic Communications 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.

### 3.2 REFERENCES:

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

### 3.3 PROCEDURES:

#### 3.3. 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.

#### 3.3. 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

#### 3.3. C. 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 medium, network drive, or print-out 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.

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

i. Legal Custodian. E-mail records shall be maintained by the City Clerk.

ii. Information Services Manager. If e-mail is maintained in an on-line data base, it is the responsibility of the Director of Planning & Development to provide technical support for the Legal Custodian as needed. When equipment is updated, the Director of Planning & Development shall ensure that the ability to reproduce e-mail in a readable form is maintained. The Director of Planning & Development shall assure that e-mail programs are properly set up to archive e-mail as required by the City Clerk.

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

### 3.3. 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.

## **SECTION 4: OTHER ELECTRONIC MEDIA**

### 4.1 ACCESS and AUTHORITY

4.1. 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.

4.1. B. The provisions of this Policy shall apply to the use of City-owned/provided equipment 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.

### 4.2. PARTICIPATION IN ON-LINE FORUMS

4.2. A. Employees 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.

4.2. 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.

4.2. C. 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 City of Stoughton.*

4.2. D. Employees should note that even with a disclaimer, a connection with the City exists and a statement could be imputed legally to the City. Therefore, employees should 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 a City-provided account. Communications must not reveal confidential information and must not otherwise violate this or other City policies.

4.2. E. 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.

#### 4.3. SOCIAL NETWORKING

Social media communication tools that facilitate interactive information-sharing, interoperability, and collaboration are useful outreach and communication tools. Commonly used social media websites include Facebook, Twitter, MySpace, YouTube, Flickr, Tumblr, and LinkedIn.

4.3. A. Definitions

i. Blog: a blog (short for web-log) is a personal online journal that is frequently updated and intended for general public consumption. Blogs are defined by their format: a series of entries typically posted to a single page in reverse-chronological order. Blogs generally represent the personality of the author or reflect the purpose of the website that hosts the blogs. Topics sometimes include brief philosophical musings, commentary on internet and other social issues, and links to other sites the author favors, especially those that support or reject a point being made on a post. There are any number of sites that act as blog-aggregators, with which users can read updates to and leave comments on the blogs of other site-users. These sites have social functions similar to Facebook and Twitter.

ii. Chat room: A way of communicating by sending text messages to multiple people in the same chat room in real-time. The term can mean any technology ranging from real-time online chat over instant messaging and online forums to fully immersive graphical social environments.

iii. Forum: An online discussion group where users can post comments and thoughts, either anonymously or as themselves, usually not in real-time.

iv. IM: Instant Messaging is a way of communicating one-on-one by sending text messages over the internet in real-time. Many social networking sites offer IM functions, frequently called Chat.

v. Personal website: Website created or configured by an individual for business, social, or entertainment purposes.

vi. Social networking site: A website or service that enables users to create public profiles within that website and form relationships with other users of the same website who

access their profile. Social networking sites can be used to describe community-based websites, online discussion forums, chat rooms, and other spaces accessed online or by cell-phone.

vii. URL: Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web. For example, <http://www.google.com> is the URL for Google: the address where Google's website can be found.

viii. Website: Any computerized document, file, or menu accessible on the Internet and/or World Wide Web.

#### 4.3. B. City of Stoughton Sponsored Sites

i. All City of Stoughton-utilized social networking sites shall be used in conformance with, and be consistent with, applicable state, federal, and local laws, regulations, and policies, including all information technology security policies. This includes any applicable records retention time periods.

ii. City-sponsored sites are only to be accessed for City-approved purposes.

iii. All content of City-sponsored must be work-related and professional in tone.

iv. City-sponsored sites must comply with all relevant aspects of the City's Electronic Communication & Information System Policy.

v. Employees shall not blur or combine their personal and professional lives when operating a City of Stoughton social networking site.

vi. All City of Stoughton-related communication through social media outlets should remain professional in nature and should always be conducted in accordance with the City's information technology policies, practices, and expectations. Employees must not use City social networking sites for political purposes, to conduct private commercial transactions, or to engage in private business activities. If an account is used for City business, the entire account, regardless of any personal views, is subject to these guidelines, including the collection and preservation provisions. Employees should be mindful that any statements made are on behalf of the City and should therefore use discretion when posting or commenting. Employees should always consider whether it is appropriate to post an opinion, commit oneself or the department to a course of action, or discuss areas outside of one's expertise. Communication should include no form of profanity, obscenity, or copyright violation. Confidential information must not be shared.

vii. Employees are required to:

a. Be respectful of all individuals and communities with which they interact online;

b. Be polite and respectful of other opinions, even in times of heated discussion and debate;

c. Adhere to the Terms of Use, and seek to conform to the cultural and behavioral norms, of the social media platform being used; and

d. Respect copyright, privacy, financial disclosure, and other applicable laws when publishing on social media platforms. Employees should check with their supervisor if they are not certain about what they can reproduce or disclose on social media platforms.

viii. When creating social media accounts for City-related professional purposes that require individual identification, City employees should use their actual names, not pseudonyms. Any employee using his or her name should be mindful of the following:

- a. They cannot assume privacy. Employees must only post information that they are authorized to disclose.
- b. They must use different passwords for different accounts (both social media and existing work accounts). Using the same password for all accounts increases vulnerability and the likelihood of all accounts being compromised.

ix. Terms of Service

Employees should be aware of the Terms of Service (TOS) of each particular form of social networking media. Each form of social networking media has its own unique TOS that regulates how users interact. Any employee using a form of social media on behalf of the City of Stoughton should consult the most current TOS in order to avoid violations. If the TOS contradicts the City's policy, then a decision should be made about whether use of such media is appropriate.

4.3. C. Non-City-Sponsored and Other Personal Social Networking Sites

City employees are allowed to have personal social networking sites under the following conditions:

- i. Personal sites must remain *personal* in nature and be used to share personal opinions and non-work related information only. Employees must maintain a distinction between their personal opinions and the views of the City of Stoughton.
- ii. Personal sites should include a disclaimer that the opinions being expressed are those of the individual and not of the City of Stoughton. A disclaimer is required when employees:
  - a. refer to work done by or for the City;
  - b. comment on any City-related issues; or
  - c. provide a link to a City website.

See Section 4.2.C for an example of the appropriate language to be used in disclaimers.

- iii. Personal sites may not be accessed using the City's technology.
- iv. Personal sites may not be accessed during work time, excluding authorized break or unpaid meal periods.
- v. Personal sites may not contain statements that are vulgar or obscene, are threatening, or which violate the City's unlawful harassment policy.
- vi. Employees should never use their City of Stoughton email account or password in conjunction with a personal social networking site.

4.3. D. Public Records

Like e-mail, communication via City-related social networking websites constitutes a public

record. This means that both the posts of the employee administrator and any feedback by other employees or non-employees, including citizens, will become part of the public record.

The City of Stoughton is subject to the State of Wisconsin Open Records Law, and as such all communication posted is subject to disclosure and retention.

#### 4.3. E. Records Management and Preservation

Communication through City of Stoughton-related social media is considered a public record.

i. All comments or posts made to City of Stoughton account walls or pages are public, not private.

ii. Employees who receive messages through the private message services offered by some social media sites should encourage users to contact them at a public email address maintained by the City. For private messages that employees do receive, they should be treated as constituent e-mails and, therefore, as public records.

The City of Stoughton assumes responsibility for public records and complies with the retention period set forth in the retention requirements schedule. The City assigns its own schedule of collection and retention for social networking websites which it maintains.

**E-MAIL AND ELECTRONIC COMMUNICATIONS POLICIES**

**EMPLOYEE NOTICE**

As an employee of the City of Stoughton (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 Department Head.

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.

\_\_\_\_\_  
Employee Name (PLEASE PRINT)

\_\_\_\_\_  
Employee Signature Date

\_\_\_\_\_  
Supervisor Signature Date

*Copy for Employee*

**E-MAIL AND ELECTRONIC COMMUNICATIONS POLICIES**

**EMPLOYEE NOTICE**

As an employee of the City of Stoughton (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 Department Head.

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.

---

Employee Name (PLEASE PRINT)

---

Employee Signature Date

---

Supervisor Signature Date

*Copy for Employee's Personnel File*