CITY OF Fremont

Office of the Mayor
3300 Capitol Avenue, Building A | P.O. Box 5006, Fremont, CA 94537-5006
510 284-4011 *ph* | 510 284-4001 *fax* | www.fremont.gov

September 15, 2015

George Phillips
Foreman
2014-2015 Alameda County Civil Grand Jury
1401 Lakeside Drive
Suite 1104
Oakland, CA 94612

Re: Response to Grand Jury Report

Dear Mr. Phillips:

The City of Fremont thanks the Grand Jury for its service in addressing the wide areas of concerns represented by the Grand Jury report for 2014-2015. It is daunting to review the various reports issued this year without being impressed by the areas of expertise the members must have developed just to tackle these varied and difficult subjects.

We thank the Grand Jury for its handling of the citizen's complaint leveled against the City of Fremont Email Retention Policy. Although we might not agree with all of the comments in the report, we are pleased that the Grand Jury did not support the first claim of the complaint being investigated: that the City of Fremont systematically destroys all City emails after a 30-day period, *alleging a violation of California law.* Neither your Findings, nor the text of the report conclude that the City's former policy violates the law or that the City destroys all emails.

The City Council, as well as the City staff, was surprised by the investigation, having had no controversy over the City's email policy in the 15 years since its adoption. Coincidentally, the City staff was reviewing the policy for potential changes before the Grand Jury informed us of the investigation. During staff appearances before the Grand Jury, the Grand Jury was informed of the planned amendment of the City policy to extend the 30-day purge cycle to 90 days. The Grand Jury was also made aware of the staff's research on the cost of various archiving systems which could provide a searchable archive for the two-year retention period of most records. On June 1, 2015, our new email retention policy took effect, dealing with both issues. It reads in relevant part as follows:

Email means any electronic text, visual or audible communication to or from any User using the Email System, including all information, data, and attachments to the communication.

1. ***The Email System shall be used for transmission of information.***
The Email System is provided by the City to Users as a convenient and efficient method of rapidly communicating information in an electronic format. Emails are automatically purged by the City pursuant to the schedule set forth below.

2. *Interface with the Public Records Act.*
All "public records" (which generally means any writing, whether electronic or paper, that contains information relating to the conduct of the public's business) are governed by the mandatory public disclosure requirements of the Public Records Act and its exceptions (Gov't. Code §§ 6250 *et seq.*). Users are required to determine whether information transmitted or received through the Email system is a record that needs to be retained. If it is the User shall transfer the information from the Email System to an appropriate records storage medium (such as archiving the Email or printing the Email on paper) as set forth in the City's Records Management Program Policy. Public Records Act requests should be handled in accordance with standard departmental policy and directives. Users with any questions related to whether an Email should be retained as a public record shall consult with their supervisor, and the supervisor shall consult with the City Attorney if there are additional questions.

5. *The Email System will be automatically purged.*
All information on the Email System is subject to automatic purging (that is, deletion) by the City, without any notice to Users, in accordance with the schedule set forth below.

a. **The retention period for calendar, tasks, and notes shall be 365 calendar days.**

b. **Effective June 1, 2015, the retention period for Email messages sent and received whether read or unread (unopened) shall be 90 calendar days. The retention period for Email items moved to the Deleted Items or Recover Deleted Items folders shall be 10 calendar days.**

c. **The City archives Email messages in a separate system (subject to acquisition and implementation). The retention period for Email messages in the archival system shall be 2 years from the original received or sent date of the Email message.**

A copy of the new Electronic Communications and Internet Use and Retention Policy is attached for your convenience.

Given that the City's amendment took effect prior to publishing of the Grand Jury report (including the confidential pre-release), it is not surprising that the policy does not meet all of the suggestions in the two recommendations of the Grand Jury report. Nonetheless, the City believes that this newly adopted policy is not only consistent with current law but also provides all of the transparency and access expected of Fremont by its community and officials.

With respect to each of the Recommendations of the Grand Jury, the City Council is required to indicate whether or not the recommendation has been implemented, will be

implemented, requires further analysis or will not be implemented. The City's responses are as follows:

Recommendation 15-18: The City of Fremont must change its Email retention policy to require that emails are stored and retained for at least two years.

The City Council agrees with this Recommendation and the City has already implemented changes consistent with the Recommendation to the extent that the undefined term "email" means emails relating to the conduct of the public's business. To the extent that the Grand Jury considers "emails" to include emails not related to the public's business such as emails containing spam, advertisements, unsolicited notices of programs and classes, or other emails not retained in the ordinary course of business, the City Council respectfully disagrees that it is required by law to retain those types of emails for two years.

Recommendation 15-19: The City of Fremont must change its email retention policy so that no emails are classified as preliminary drafts, but rather that all such emails are retained in the regular course of business and subject to the Public Records Act.

The City Council agrees with this Recommendation and the City has already implemented changes consistent with the portion of the Recommendation regarding classification of emails as preliminary drafts. It disagrees if the Grand Jury includes in "all emails" those not related to the public's business such as emails containing spam, advertisements, unsolicited notices of programs and classes, or other emails not retained in the ordinary course of business.

With respect to each of the Findings of the Grand Jury, the City Council is required to indicate its agreement, partial agreement or disagreement. The City's responses are as follows:

Finding 15-22: The City of Fremont's classification of emails as preliminary drafts deprives the public of key opportunities to oversee government operations.

The City Council notes that the current policy does not classify emails as preliminary drafts. Further, the City Council finds no evidence in the Report to suggest that the former policy deprived any person or organization of any opportunity to oversee Fremont's operations. The City Council is not aware of any instance in which a Public Records Act request was denied on the grounds that emails constitute "preliminary drafts." To our knowledge, Emails that were retained as public records in the ordinary course of business have routinely been provided in response to requests for public records. Furthermore, training regarding the identification, retention and disclosure of public records is routinely provided to City staff in various formats.

Finding 15-23: The City of Fremont's classification of emails as records not kept in the regular course of business, unless specifically saved, deprives the public of important opportunities to monitor government.

The City Council notes that the current policy does not classify emails "as records not kept in the regular course of business, unless specifically saved". Further, the City Council finds no evidence in the Report to suggest that the former policy deprived the public of important opportunities to monitor government. Apparently, the Grand Jury assumes that City staff in Fremont failed to meet their obligations to save all emails, outside of the email system, that were in fact records for the purposes of the Records Retention Act. The City Council is not aware of any evidence to support this conclusion.

Policy Section 5c notes that a separate system for archiving emails for two years remains to be acquired. We expect that acquisition will be brought before the City Council and approved before the end of calendar year 2015.

The City Council again thanks the Grand Jury for its diligent service.

Sincerely,

Bill Harrison

Bill Harrison
Mayor

cc: Vice Mayor Chan
Councilmember Bacon
Councilmember Mei
Councilmember Jones
City Manager
City Attorney

CITY OF Fremont	ADMINISTRATIVE REGULATIONS	NUMBER: 1.14	PAGE 1 of 12
		REVISION: 3	SUPERSEDES: 3/4/2009
SUBJECT: ELECTRONIC COMMUNICATIONS AND INTERNET USE AND RETENTION		APPROVED BY: Fred Diaz City Manager	EFFECTIVE DATE: June 1, 2015

I. OVERVIEW AND PURPOSE

To provide guidance to City officers and employees (Users) for the use of the City's Electronic Communications Systems (including the E-Mail system) and use of the Internet for work purposes and to establish retention requirements for electronic messages.

II. POLICY

It is the general policy of the City of Fremont that use of the City's Electronic Communication Systems and the Internet are limited to official City purposes. The City's equipment and systems should be used for City of Fremont business only, except as otherwise provided below or approved by an employee's department director. Users are expected to use the City's technology in a professional and appropriate manner that supports the efforts of the City and does not diminish productivity. The City's E-Mail and communications systems may not be used to solicit or persuade others for commercial ventures, religious or political causes, outside organizations, criminal activity or other non-job related solicitations. All information stored or transmitted on City equipment and systems is the property of the City and may be accessed by the City at any time; Users have no individual privacy rights to any such information. Any violation of this regulation may result in disciplinary action, up to and including termination.

III. DEFINITIONS

A. **Electronic Communication** means any kind of communication created by, retrieved by, sent to, or stored by any User on City servers, whether on-premise or hosted by a third party, using any Electronic Communications System, including all information, data, and attachments to the communication.

B. **Electronic Communications System** means the system of City-owned devices (including hardware, software, and other equipment) used by the City for the purpose of facilitating the transmission or storage of electronic information such as Internet communications, the electronic mail (E-Mail) system (including folders such as Inbox, Sent Items, Deleted Items, Recover Deleted Items, Calendar, Notes, and Tasks), voice mail system (including chat), telephones, pagers, radios, computers, smart mobile devices (such as smartphones and tablets), cellular telephones including text messaging, other wireless E-Mail devices, and all peripheral devices such as hard drives, disks, flash drives, tapes, film, DVDs and CDs.

C. **E-Mail** means any electronic text, visual or audible communication to or from any User using the E-Mail System, including all information, data, and attachments to the communication.

D. Internet means an interconnected system of networks that connects computers around the world via the TCP/IP protocol.

E. Personal Electronic Device means any electronic device such as a pager, cell phone, smart mobile device (smartphone, tablet), laptop, or wireless Internet device that is solely owned by a User and may or may not be used to fulfill duties for the City of Fremont.

F. Records Management Program Policy means the City's Records Retention and Disposition Policy, as set forth in Resolution No. 2 004-24.

G. User means all classified and unclassified employees, temporary, part-time employees, contract workers, supervisors, managers, department directors, volunteers and appointed and elected officials.

H. Virtual Private Network (VPN) is a network that uses a public telecommunications infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

I. Web Access means the access of the City's E-Mail system from any location other than the User's assigned desktop or laptop installed at City facilities.

J. Wireless Access Point means zones throughout the City of Fremont that provide Internet or E-Mail services to a wireless device in order to make the completion of City business more effective and efficient.

IV. POLICY IMPLEMENTATION

A. Electronic Communications System

1. *Information on the Electronic Communications System is not private.* The Electronic Communications System and all Electronic Communications are the property of the City. The City has the right, but not a duty, to inspect or audit any and all Electronic Communications, at any time, for any lawful purpose, without notice to any User. Accordingly, no User shall have any expectation of privacy regarding the content of any Electronic Communication. Users should also be aware that access to Internet sites from City computers leaves an electronic trail which may be traced back to a City computer or user.

2. *The Electronic Communications System and the Internet shall be used in a professional manner.* In the use of the Electronic Communications System and the Internet, Users shall comply with all relevant City regulations including, but not limited to the City's "Harassment, Discrimination, and Retaliation Policy and Procedure," (Administrative Regulation 2.12). Other inappropriate and prohibited uses of the Internet include, but are not limited to the following:

    1. Threats
    2. Slander/Libel
    3. Defamation

4. Obscene, suggestive or offensive graphic images or messages, including any access of pornographic materials.
5. Political endorsements
6. Private, for profit activities
7. Use of software not required for City business including games or other entertainment software
8. Criminal activity

Users shall prepare Electronic Communications in a lawful, ethical, professional, and businesslike manner. The use of the Electronic Communications System and the Internet is a privilege which may be revoked by the City at any time.

3. *Users shall protect the security of the Electronic Communications System.* Users shall make all reasonable and necessary efforts to: protect the confidentiality of information which is placed in their control or care, minimize the likelihood of inadvertent transmission of confidential information to unintended recipients, prevent unauthorized intruders from accessing the Electronic Communications System, and prevent the introduction or spread of computer viruses. **For the communication of sensitive and confidential information, Users shall minimize the use of E-Mail and maximize the use of alternative communication media (such as face-to-face conversations, telephone, and hard copy memos).**

4. *Occasional and limited "personal" use of the Electronic Communications System* is allowed (no more than 10 minutes during an employee's working hours) when the use does not: (1) interfere with the User's work performance, (2) interfere with the work performance of any other User, (3) unduly impact the operation of the Electronic Communications System, (4) support a User's personal commercial endeavors, or (5) violate any other provision of this Regulation, any other City policy, or legal requirement. In addition, subject to the discretion of the supervisor, a User may engage in personal use of the Electronic Communications System during non-working hours (i.e., lunch time) if their work station is not within the public's view and the use does not violate any of the factors noted above.

B. E-Mail System

1. *The E-Mail System shall be used for transmission of information.* The E-Mail System is provided by the City to Users as a convenient and efficient method of rapidly communicating information in an electronic format. E-Mails are automatically purged by the City pursuant to the schedule set forth below.

2. *Interface with the Public Records Act.* All "public records" (which generally means any writing, whether electronic or paper, that contains information relating to the conduct of the public's business) are governed by the mandatory public disclosure requirements of the Public Records Act and its exceptions (Gov't. Code §§ 6250 et seq.). Users are required to determine whether information transmitted or received through the E-Mail system is a record that needs to be retained. If it is, the User shall transfer the information from the E-Mail System to an appropriate records storage medium (such as

archiving the E-Mail or printing the E-Mail on paper) as set forth in the City's Records Management Program Policy. Public Records Act requests should be handled in accordance with standard departmental policy and directives. Users with any questions related to whether an E-Mail should be retained as a public record shall consult with their supervisor, and the supervisor shall consult with the City Attorney if there are additional questions.

3. *Automatically forwarding business-related E-Mails from Users' City E-Mail accounts to their personal E-Mail accounts is not allowed.* Users are also prohibited from forwarding business E-Mails containing confidential information. Users are cautioned that any business E-Mail forwarded to a personal account may subject that personal account to a Public Records Act request.

4. *Routine backup of the City's E-Mail System is intended for disaster recovery only,* which does not allow individual E-Mails that are automatically purged to be restored.

5. *The E-Mail System will be automatically purged.* All information on the E-Mail System is subject to automatic purging (that is, deletion) by the City, without any notice to Users, in accordance with the schedule set forth below.

    a. The retention period for calendar, tasks, and notes shall be 365 calendar days.

    b. Effective June 1, 2015, the retention period for E-Mail messages sent and received whether read or unread (unopened) shall be 90 calendar days. The retention period for E-mail items moved to the Deleted Items or Recover Deleted Items folders shall be 10 calendar days.

    c. The City archives E-Mail messages in a separate system (subject to acquisition and implementation). The retention period for E-Mail messages in the archival system shall be 2 years from the original received or sent date of the E-Mail message.

6. *Do not bypass the automatic purge cycle.* Users shall not manipulate settings in the E-Mail System in an attempt to bypass the automatic purge cycle set by the City. This is not to preclude Users from deleting E-Mails earlier than the purge cycle period.

7. *All User E-Mails.* The E-Mail System is capable of simultaneously transmitting information to "All Users" of the E-Mail System, or all E-Mail Users in a building ("All Building"). All User or All Building E-Mail or voice mail messages require approval by the User's department director.

8. *Do not attempt to disguise the origin of an E-Mail.* No User shall attempt to disguise the origin of any E-Mail, unless authorized by the Chief of Police for a criminal investigation.

9. *Do not access other Users' E-Mail.* No User shall access, or attempt to access, another User's E-Mail unless authorized by: (1) the other User, or (2) the other User's supervisor, or (3) the City Manager.

10. *Remote access to the City's E-Mail System and network.*

    a. Access to the City's E-Mail System using an Internet web browser from a non-City device is limited to exempt employees, with exceptions granted by the department director or designee.
    b. Remote network access through a virtual private network (VPN) is restricted. **Users must have prior written approval from their department director, or designee, in order to access the City's network remotely through a User's Internet Service Provider. Generally, such access will be limited to exempt employees, with exceptions granted only by the department director.**
    c. Users who access the City's E-Mail or network remotely are responsible for ensuring that any non-City device used to establish a connection is properly secured, running all necessary operating system and software patches, and anti-virus software.

11. *Mobile device access.* Exempt employees may be permitted to access City E-Mail or other systems using a City or personally-owned mobile device with a VPN, Internet, Microsoft ActiveSync, or other connection. The employee's department director, or designee, and the Information Technology Services Director approvals are required for non-exempt employees to have such access on their personal mobile devices.

C. Internet Use and Wireless Access

1. *The Internet shall be used for City-related business only* and must be used appropriately at all times.

    a. Copyright laws regarding protected commercial software or intellectual property shall be honored.

    b. Use of the Internet should be minimized so that unnecessary network traffic will not interfere with others in using this shared network resource. This includes the use of the Internet for the storage of files for purposes such as backup.

    c. If it is necessary to download applications or programs from the Internet, Users must contact the Infrastructure Services Manager, or designee, for instructions on downloading procedures and authorization to proceed in order to prevent infection of the City's local network by computer viruses.

    d. Exchanges of information, such as list serves, allow topic-specific research and enable communication with a larger topic-specific audience with shared interests and therefore are considered an appropriate use of the Internet.

e. All Users are prohibited from using the Internet for any unlawful purposes, including unauthorized use of a protected/secured resource of any department of the City.

f. All Users are prohibited from using the Internet for the transmission of unprofessional communications not associated with normal work responsibilities or using City resources for unsolicited advertising for personal gain.

g. All Users are prohibited from browsing the Internet, posting messages on bulletin boards, or participating in chat rooms, except for City related business.

h. Occasional and limited "personal" use of the Internet is allowed (no more than 10 minutes during an employee's working hours). Subject to supervisor approval, a User may also use their City-provided Internet access for personal needs during non-working hours (i.e., lunch time) if the work station is not within the public's view. Such usage must not interfere with the User's performance of duties or violate any of the factors noted in Section IV (A) 2.

i. Users are forbidden at all times from using City equipment or Internet access for private, for-profit activities.

2. *Internet usage is subject to oversight.* In order to protect the City's interest, the Information Technology Services Department may monitor and log individual use of the Internet for system integrity and maintenance in order to detect and prevent fraud, abuse and unlawful usage. All persons using the City's Internet and other Electronic Communications Systems consent to the monitoring of all data, files, messages and other transmissions passing through the Internet, both outgoing and incoming.

3. *The City reserves the right to block access to any Internet sites which are determined to be non-applicable for City-related business.* Petition for access to restricted Internet sites shall be made in writing to the Information Technology Services Director with written authorization by the User's department director. Access may be granted if access to the Internet site is necessary and appropriate for City-related business, as determined by the City Manager or designee.

4. *Wireless Access Points.* Several Wireless Access Points have been installed throughout the City for access to the Internet. This convenience shall only be used to conduct City business and is not intended for personal usage.

D. Voice Mail System

A voice mail box is set up for a User's extension on the City's telephone system. Voice mail stored on the City's voice mail system is also deemed business related and, as such, is subject to oversight and may be monitored. The voice mail system will store up to a maximum of 30 messages for each User. All information in the voice mail system is subject to automatic purging (deletion) by the City, without any notice to Users, in accordance with the schedule below.

1. Voice mail messages that have not been listened to are purged every 30 calendar days.

2. Voice mail messages that have been played (listened to) are purged every 15 calendar days.

3. Voice mail messages in WAV file format that are attached to E-Mail messages are retained and purged according to the E-Mail retention periods specified in Section B-5 of this Policy.

E. Personal Electronic Devices

1. The City is aware that we live in a time that most of our Users are electronically connected in one form or another, usually by smartphone, tablet, cell phone, pager, or other wireless mobile device. A User may use a personal electronic device in the workplace on an incidental basis. Excessive (more than 10 minutes during work hours in a workday) personal use of such devices is prohibited.

2. Excessive use of personal electronic devices by a User or use which violates City policies and regulations could result in disciplinary action.

3. Synchronizing a City E-Mail account for exempt employees to a personally owned electronic device so that all E-Mail messages or calendar appointments sent to the User's City E-Mail account are forwarded to the personal electronic device is permitted. The User's department director's, or designee's, approval is required to synchronize a non-exempt employee's e-mail account (both e-mail and calendar or calendar only) to a personally-owned electronic device. However, the User should be aware that this information may be subject to the Public Records Act and may be accessible to the City. There should be no expectation of privacy for work related communications sent or received by a personal electronic device.

F. Remote Access to City Resources

Under various labor laws and labor memorandums of understanding, employees of the City, other than FLSA exempt employees, must be compensated with overtime pay for any work performed outside of normal duty hours, regardless of the time of day or day of week. Therefore, any work performed outside normal work hours by such employees must be approved in advance by the employee's supervisor. If employees are unsure whether they are exempt or non-exempt, they should ask

their supervisor to explain their status before remotely accessing the City's electronic communication resources unless authorized by their supervisor.

1. Non-exempt employees may not remotely access the City's electronic communication resources for any purpose outside of normal work hours other than for resolving scheduling questions or other trivial use as previously described in this Policy.

2. Remote access to the City's self-service applications is allowed for employees. One specific self-service application is the payroll and benefit management system where employees can review or print paycheck stubs or W-2's for their own purposes and to review or change benefit or other personal information. Use of the payroll and benefit management system, and similar systems, by non-exempt employees outside of the employee's duty hours does not qualify for overtime compensation. Non-exempt employees may not use the self-service payroll system to prepare time cards outside of normal work hours unless approved by the department director or designee.

3. All overtime work performed through remote access to the City's electronic communication resources must be reported on the non-exempt employee's time sheet during the pay period in which the overtime was earned.

4. Employees may not access the City's electronic communication resources remotely with the intention of waiving their right to overtime compensation. That right cannot be waived under the terms of the labor laws and labor memorandums of understanding and is forbidden by this Policy.

G. Collaboration Software

Collaboration software (e.g. GoToMeeting) is often used when vendors want to see the User's workstation to provide support or updates and to present information to City employees using a City workstation in a general purpose room (such as a conference or training room). This type of software is permitted provided that the User approves and is present throughout the entire session. The User is responsible for the necessary precautions to make sure unrelated data and applications are not accessible to the third party accessing the User's or general purpose room's workstation. Third party access outside the User's or general purpose room's workstation is not permitted without authorization by the Information Technology Services Department.

V. PROTECT CONFIDENTIAL INFORMATION

Whenever a User possesses confidential information, the User has an obligation to take all reasonable and necessary steps to protect the confidentiality of the information and to minimize the likelihood of inadvertent transmission of the confidential information to unintended recipients. If a User has any question regarding the implementation of this section, contact the City Attorney's Office.

A. Determine if the information is "confidential." Users shall treat all information as "confidential" if there is any possibility that the information could be considered

personal (such as personnel or medical records), or private (such as proprietary or financial information received from a third party), or if it could potentially expose the City to liability, or if it falls within one of the categories identified in section V., paragraph D. of this Regulation.

B. Identify the people who are authorized to receive the confidential information. Users with the care and custody of confidential information shall be responsible for determining which other Users (or possibly private attorneys or consultants hired to represent the City) are authorized recipients of the information. Generally, only people with a "need to know" the confidential information are authorized recipients. Users with any questions as to who is an authorized recipient for confidential information shall contact the City Attorney's office. Do not communicate confidential information to any person other than an authorized recipient. Do not forward a confidential E-Mail to any unauthorized recipient. Exercise care when using distribution lists to make sure all addressees are appropriate recipients of information. Ensure you know who is included on a list before transmitting. Do not discuss confidential information outside of the workplace.

C. Consider the availability of alternate means of communication. When it is necessary to communicate confidential information, Users shall consider the risks and benefits of all available means of communication (including: face-to-face communications, telephone, E-Mail, fax, or hard copy memo), and Users shall use a means of communication which minimizes the risk that the confidential communications will be received by an unintended recipient (that is, a person who does not "need to know" the confidential information). For confidential information which is particularly sensitive (for example, highly personal medical information, or information which could expose the City to significant liability), Users shall exercise a heightened sense of care in protecting the confidentiality of the information.

D. Minimize the use of E-Mail for confidential communications. For the communication of confidential information, Users shall minimize the use of E-Mail and maximize the use of alternative communication media. In determining whether or not confidential information should be communicated using E-Mail rather than some other form of communication, each User shall weigh the benefits of communicating using the E-Mail System (including speed of communicating in writing over great distances and the efficiency of electronic editing of documents by one or more people) against the risk that the confidential information may be inadvertently sent or forwarded to an unintended recipient.

E. Clearly identify all confidential writings. All confidential information that is contained in an Electronic Communication shall be clearly marked CONFIDENTIAL.

VI. RESPONSIBILITIES

A. Users are required to:

1. Adhere to his or her department's own operating procedures with emphasis on addressing security concerns in accordance with the policy guidelines of this regulation.

2. Properly manage individual E-Mail accounts consistent with the Policy herein described.

3. Immediately report any potential criminal activity involving the use of any Electronic Communication to his or her immediate supervisor, manager, or department director.

4. Use Electronic Communications Systems and the Internet in compliance with this Policy. If unsure as to whether a contemplated activity or course of conduct constitutes a violation of this Policy, request clarification from his or her immediate supervisor, manager, or department director.

5. Acknowledge receipt and understanding of this Policy annually.

6. For questions regarding the implementation of this Regulation, contact their supervisor or either:

   a. the City Attorney's Office for legal questions, such as an interpretation under the Public Records Act;

   b. the City Clerk's office regarding the Records Management Program Policy; or

   c. the Information Technology Services Department regarding any technical issues related to the use of any Electronic Communications System, remote access to the City's E-Mail System or network, or wireless access point.

B. Supervisors/Managers/Department Directors, in addition to the responsibilities listed above for individual Users, are required to:

1. Be responsible for managing Internet usage in their area of responsibility.

2. Be knowledgeable about this Policy and model behavior that complies with the principles and guidelines of this Policy.

3. Implement and communicate this Policy to employees, answer any questions and provide guidance to employees regarding appropriate use of Electronic Communications Systems and the Internet to ensure employees understand and adhere to the regulations in this Policy.

4. Provide a copy of this Policy and review it annually with each employee.

C. Information Technology Services Department is required to:

1. Coordinate enhancements of Electronic Communications Systems and Internet services, including hardware and software modifications.

2. Implement strategies to enhance effective Internet use, including User training.

3. Develop in-house architectures that allow for sharing data, department applications, networks and host computers. Also, support standards for internal networks and for interagency communications.

4. Monitor use of the Internet by department and provide that information to department directors on a consistent schedule.

VII. REMEDIAL AND DISCIPLINARY ACTION

Any User determined to have violated this Policy may be subject to appropriate disciplinary action, up to and including termination. In addition, a User may have his or her access to City Electronic Communication Systems (such as computer files, Internet, and E-Mail) limited or revoked.

ACKNOWLEDGMENT

This is to acknowledge that I have received and read a copy of the Electronic Communications and Internet Use and Retention Policy, Administrative Regulation 1.14.

I understand that failure to follow the provisions of the guidelines could lead to disciplinary action up to and including termination. I further acknowledge that this document will be placed in my personnel file.

(Supervisor signature)	(Employee/User signature)
(Print name)	(Print name)
(Date)	(Date)