The City of Philadelphia provides access to an electronic mail (“e-mail”) system to help you do your job faster and smarter, and be a well-informed business citizen. The facilities to provide that access represent a considerable commitment of City resources for telecommunications, networking, software, storage, etc. This Electronic Mail Policy is designed to help you understand our expectations for the use of those resources and to help you use those resources wisely.

While we’ve set forth explicit requirements for e-mail usage, we would like to start by describing our email usage philosophy. First and foremost, all electronic systems, hardware, software, temporary or permanent files and any related systems or devices used in the transmission, receipt or storage of e-mail are the property of the City. E-mail messages are considered to be City property and may be retrieved from storage even though deleted by the sender and receiver. E-mail communications that qualify as public records are the property of the record creating office and are regulated by and managed with assistance from the Department of Records.

To be absolutely clear on this point, all existing City policies apply to your conduct on the e-mail system, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of City resources, sexual harassment, information and data security, and confidentiality.

E-mail communications should be drafted with the same care and formality as a printed or handwritten memorandum. They should not contain informal remarks that are potentially embarrassing or offensive to City personnel or to any other person. The use of City e-mail systems is subject to all applicable laws and City policies prohibiting infringement of intellectual property rights, harassment, discrimination, and defamation.

The attached Electronic Mail Policy was reviewed and revised by the Information Technology Security Steering Committee, established by the Mayor’s Executive Order No. 2-97. This policy is being distributed to all City employees granted e-mail access through City facilities.

Please review the attached Policy; if you do not fully understand the terms of this policy or have concerns with abiding by these terms, you can contact the IT Security Manager at the Mayor’s Office of Information Services at 686-8171.

CITY OF PHILADELPHIA
ELECTRONIC MAIL POLICY
Revised August, 2004

This policy applies to all users of the City of Philadelphia (“City”) electronic mail (“e-mail”) systems and provides guidelines for use of the City’s email system.

I. OWNERSHIP

All electronic systems, hardware, software, temporary or permanent files and any related systems or devices used in the transmission, receipt or storage of e-mail are the property of the City. E-mail messages are considered to be City property and may be retrieved from storage even though deleted by the sender and receiver. E-mail communications that qualify as public records are the property of the record creating office and are regulated by and managed with assistance from the Department of Records. Departmental records retention schedules will be made available to employees. These schedules are for internal city use only and employees may not distribute them (verbally, electronically, in writing, or by any other means) to any person who is not a City employee under penalty of disciplinary action.

II. GUIDELINES FOR USE

(1) E-mail communications should be drafted with the same care and formality as a printed or handwritten memorandum. They should not contain informal remarks that are potentially embarrassing or offensive to City personnel or to any other person.

(2) Use of City e-mail systems is subject to all applicable laws and City policies prohibiting infringement of intellectual property rights, harassment, discrimination, defamation, and illegal activity. You may not use e-mail for communications or transfers of information or data that:

- Infringe the copyright, trademark, or other intellectual property rights of third parties (this includes communications and transfers that contain copyrighted materials, such as articles, books, photographs, and graphical images, in violation of copyright law);
- Are otherwise illegal or wrongful or contrary to the established policies of your agency or the City;
- Contain language that is defamatory, fraudulent, harassing, offensive, hostile, illegal, or discriminatory including, but not limited to, the display or transmission of sexually explicit images, cartoons, jokes, messages, chain letters, or other materials, which activities are governed by the attached City of Philadelphia Personnel Department Policy for Preventing Sexual Harassment in City Government.

The City recognizes, however, that certain employees may have valid business reasons to use the e-mail system to transmit or access otherwise inappropriate materials in the course of performing their duties. (Examples include, but are not limited to, criminal or administrative
(3) Anyone who has your password can access your e-mail. You are responsible for maintaining the security of your individual e-mail account. You should never publicize or reveal your password to others who are not authorized by your agency or the City to know your password, or share e-mail accounts with other users except as authorized by your supervisor. (If you need to share data residing on your computer with others, you should use message forwarding and attachment functions in e-mail, public directories on local area networks, and other authorized information-sharing mechanisms.) You should choose passwords that are difficult to guess (not, for example, a dictionary word, personal detail, or word reflecting work activities). You should use passwords that mix letters and numbers because they are more difficult to guess than words or letters alone. If you are going to be away from your computer for more than a few minutes, it is advisable to exit the e-mail program. If you leave your computer on with the e-mail program open, anyone can read your messages or send messages bearing your account name. You may be held responsible for communications sent by persons to whom you have intentionally disclosed your password.

(4) Software downloaded to City computers from non-City computers or networks via the e-mail system (e.g. through e-mail to and from Internet e-mail addresses) may contain computer viruses or otherwise interfere with the operation of your computer or the operation of City networks, including City Net. Use of City software is restricted by the terms of the applicable license and may not be made available for use by others. For these reasons, you may not knowingly use e-mail to download software from the Internet or transfer software to others without the approval of your agency’s Director of Management Information Systems (“MIS Director”).

(5) You may not encrypt e-mail messages or files without the approval of the Mayor’s Office of Information Services (“MOIS”). You may be required to furnish copies of the encryption key(s) to MOIS as a condition of such approval unless you can demonstrate a legitimate business need for confidentiality and security.

(6) You should not store large numbers of e-mail messages in your in-box. Retaining messages consumes storage space on the network server and can affect performance. Check your in-box daily and delete unwanted messages which do not qualify as public records immediately. If the message should be retained as a public record (see Section V below), archive it as a public record within a week of receipt or creation.

(7) The e-mail system is a resource provided by the City and your agency for use by City employees in performing job responsibilities and to enhance the ability to conduct the City's business. Communication that is job-related fulfills these purposes and constitutes proper use. E-mail should be used only in connection with the conduct of City business; it should not be used for personal matters or non-City business matters.

III. PRIVACY

1. The e-mail system and the messages sent and received on it are the property of the City. Users of the e-mail system should not expect or assume privacy or any right to privacy with respect to any e-mail communication.

In order to ensure the reliability of City networks and the e-mail system, the City monitors the volume of e-mail traffic entering and leaving City networks, including the addresses of senders and recipients, and promptly investigates excessive e-mail activity on the part of individual users. E-mail is received and stored on agency and City network servers as well as individual desktop computers. Authorized staff who maintain and administer the networks and authorized managers may access or disclose the stored e-mail messages and files of City employees in the course of carrying out their authorized duties; and the City may monitor, review and disclose stored e-mail messages, without prior notice to the user, for accounting purposes, to assure proper use of e-mail, to prevent security violations, to investigate excessive e-mail activity as described above, or for any other reason deemed appropriate by the City.

Such monitoring and review of an individual employee’s e-mail messages may be done at the request of the appointing authority or designee, the Inspector General, or other appropriate City agencies, with the approval of the Mayor’s Office of Information Services. Although you delete e-mail messages from your desktop computer, they may continue to exist on network back-up or archival storage devices or on other systems beyond your control, and may be accessed even after you use the delete function.

In addition, e-mail and all other electronic communications, like paper documents, may be subject to the disclosure provisions of the Commonwealth of Pennsylvania’s Right to Know Act, the public records provisions of the Philadelphia Home Rule Charter, or both; are subject to discovery during litigation; and may be disclosed to or accessed by law enforcement authorities in the course of carrying out their official duties.

2. Departments for which confidentiality is critical to the delivery of services or the maintenance of client relationships, or is required by applicable law or regulation, will, to the maximum extent feasible, be provided with secure technology and software to ensure the confidentiality of department/client communications and transactions. Implementation of such technology and software is at the sole discretion of the City.

IV. CONFIDENTIAL INFORMATION

All users of the e-mail system are instructed to exercise greater caution in transmitting confidential information by e-mail than with other means of communication because it is easier to redistribute such information by e-mail. Confidential information should not be transmitted or forwarded to other employees within the City, or to individuals not employed by the City, who do not need and/or are not authorized to know the
information. Confidential information includes, but is not limited to, the following: personal information about employees (such as home addresses, phone numbers, and personal family information); information from any employee’s personnel file; information relating to legal proceedings involving the City; any communication between a City employee and any attorney in the Law Department; information relating to any competitive City procurement of goods or services which, if disclosed, would give a competitive advantage to one vendor over another; information related to location or price of property the City may buy; trade secrets, commercial or financial information of outside businesses; anyone’s social security number; confidential management or financial information or reports. Other kinds of information may be considered confidential by your agency, department, or a local office within your agency. If you are not certain whether information is confidential, consult with supervisors.

E-mail messages that contain confidential information should display a confidentiality notice that includes substantially the following:

“THIS MESSAGE CONTAINS CONFIDENTIAL INFORMATION OF THE CITY OF PHILADELPHIA. UNAUTHORIZED USE OR DISCLOSURE IS PROHIBITED.”

All e-mail messages to attorneys in the Law Department seeking legal advice, or relating to an attorney's legal advice, should have the following notice at the top of the e-mail message:

"ATTORNEY-CLIENT COMMUNICATION; PRIVILEGED AND CONFIDENTIAL."

E-mail messages written by Law Department attorneys, or by City employees who are attorneys acting in their capacity as attorneys, should include a confidentiality notice approved by the Law Department.

In order to preserve the attorney-client privilege, messages to and from attorneys in the Law Department or otherwise acting as attorneys for the City should never be sent to distribution lists or forwarded to anyone else within or outside the City.

V. RECORDS MANAGEMENT

Many e-mail messages created by City employees have the status of public records under Section 5-1100 of the Philadelphia Home Rule Charter and Mayor's Executive Order No. 6-92. A Records Retention Schedule has been established for each City agency or department by the Department of Records, which has responsibility under the Charter for maintaining the City’s public records and authorizing their destruction. The Records Retention Schedule identifies, by type and content, categories of document that must be retained and the period of time each category must be retained. There is no difference, for purposes of records retention and management, between paper records and documents, and electronic records and documents, including e-mail messages and attachments. If an e-mail communication and/or attachment falls within a record type identified in your agency’s Schedule, the e-mail must be saved for the period of time provided in the Schedule and destroyed (deleted) when that time has expired. Before deleting any e-mail message, you should make a determination whether the message constitutes a public record under your agency’s Records Retention Schedule, and if it does, delete or retain the message in accordance with the requirements of the Schedule for records of similar type and content. Where retention is indicated, you may use the e-mail program’s archiving function to save the record on your hard disk. If you need assistance with the determination, please contact the Records Department or the designated records management officer for your agency. Each agency is responsible for making the agency’s Records Retention Schedule available to its e-mail users and for enforcing the Schedule. Guidelines for managing e-mail messages, including retention and deletion, are available from the Department of Records.

VI. COMPLIANCE

Violations of this policy may result in restriction or loss of your e-mail privileges and are subject to the normal disciplinary procedures of your department. Any disciplinary action will be consistent with current bargaining agreements for represented employees.

VII. REVISIONS

The Mayor’s Office of Information Services has promulgated and is responsible for maintaining and updating this policy. The City of Philadelphia reserves the right to revise this policy at any time and for any reason. Communications regarding the policy should be addressed to MOIS (Attn: Chief Information Security Officer.)