



City of Pittsburgh
Operating Policies

Electronic Communications Policy	Original Date: 1/2003
	Revised: 3/1/2016

PURPOSE: To inform City of Pittsburgh employees of 1) the expected guidelines and requirements for using their email and other electronic communications provided by the City, 2) instances of prohibited use, 3) how to handle confidential electronic information, and 4) allowable hardware and software installations.

The Department of Innovation & Performance follows the City of Pittsburgh's Electronic Communications Policy. Please click this link for the City's Electronic Communications Policy.

POLICY STATEMENTS:

The City of Pittsburgh provides electronic and telephone communications, including E-mail, Internet/Intranet, voicemail and other systems to its designated employees for their use in performing their duties for the City at the City's expense. It is City policy that the electronic communications systems are to be used for principally work related purposes. Any employee who uses these systems in a manner inconsistent with this policy or in violation of any other Departmental, Bureau or City policy may be subject to disciplinary action up to and including termination. All employees who use City electronic communications systems shall certify that they have read and fully understand the contents of this policy. Any and all opinions communicated through use of these systems, whether implied or expressed, shall be those of the individual user and are not necessarily the opinions of the City or its management.

Use of City's Electronic Communications Systems:

City employees may use the City's electronic communications systems for performing lawful City business. Limited, occasional, or incidental use of electronic communication systems for personal, non-business purposes is permitted under the following conditions:

- Personal use is limited to break or lunch time.
- Personal use may not interfere with the productivity of the employee or his or her co-workers.
- Personal use may not involve any prohibited activity described in the City handbook.
- Personal use may not delay or disrupt the performance of City business.
- Personal use may not consume City resources or otherwise deplete system resources available for business purposes.

If the personal use of the City's electronic communications systems results in a cost to the City, the cost must be reimbursed by the employee.

- The City reserves the right to delete any electronic communication received by a City employee through the City electronic communications system in order to maintain the effective and efficient operation of the City's system. Deletion may occur at any time with or without prior notification. All Internet data that is composed, transmitted, and/or received by City computer systems is considered to belong to City and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.
- The equipment, services, and technology used to access the Internet are the property of the City and the City reserves the right to monitor Internet traffic and monitor and access data that is composed, sent, or received through its online connections.
- All sites and downloads may be monitored and/or blocked by the City if they are deemed to be harmful and/or not productive to business.

Procedure for Distributing Department-wide and City-wide E-mail:

- No City employee shall distribute department-wide e-mail without prior approval from his or her Department Director or Bureau Chief. Department Directors and Bureau Chiefs may distribute department-wide E-mail at their discretion.
- No City employee shall distribute City-wide E-mail. Requests for the distribution of City-wide E-mail must be made through the employee's Department Director or Bureau Chief. If the Department Director or Bureau Chief approves City-wide distribution, then he or she shall distribute the E-mail to City Department Directors and Bureau Chiefs who may forward the City-wide E-mail to the employees under his or her direction.

Prohibited Use:

It is the responsibility of each City employee to use the City's electronic communication systems in a professional and courteous manner. The City forbids use of its electronic communication systems in a manner that violates any law, regulation, ordinance, policy or procedure of the City. Examples of forbidden communications include, but not limited to, ethnic or racial slurs, sexually explicit materials (photographs, videos, drawings, etc.), messages or jokes/cartoons, unwelcome propositions or love letters or any other transmission that violates the City's No Discrimination/No Harassment/No Retaliation and Reporting Procedure, which is incorporated herein by reference. City employees shall use the same professional courtesy in E-mail communications as in used in other verbal or written communications.

City employees are prohibited from accessing without authorization or tampering with the security of computer/network equipment, files, or E-mail records of any employee. Any attempt to bypass City computer/network security controls is forbidden. Electronic "snooping" to satisfy curiosity about other employees is forbidden.

Employees should not expect privacy:

All City communications systems, hardware, software, temporary/permanent files, and any related systems or devices used in the transmission, receipt, or storage of E-mail/Internet/Intranet information are City property. The City retains the right to access information transmitted or stored on City electronic communications systems with or without prior notice to employees. Employees should not have any expectation of privacy with respect to any use, professional or personal, of the City's electronic communications systems.

Confidential information must be handled properly:

Avoid using electronic communications systems to send confidential, privileged, and/or sensitive information. Employees must exercise a much greater degree of caution in transmitting confidential information by E-mail and/or the Internet/Intranet, because of the reduced effort that is required to redistribute such information (i.e. at the touch of a button). Confidential information must never be transmitted to anyone who is not authorized to know or receive such information.

Some examples of information which may be considered confidential include, but are not limited to:

- Information from a personnel file (for example: Social Security number, personal and/or family information, address and telephone information).
- Private correspondence of elected officials.
- Information that, if released, would give a competitive advantage to one competitor or bidder over another.
- Information related to legal advice, questions, proceedings, or proposed legislation.
- Information related to the regulation of financial institutions or securities.
- Trade secrets, commercial or financial information of outside businesses.

Confidential information must never be transmitted to anyone who is not authorized to know or receive such information.

Hardware/Software Installations:

Installation of hardware/software and/or utilities that have not been sanctioned as set forth by the Department of Innovation & Performance will be removed at any time without notice, and the installing employee may be subject to disciplinary action by their department head. The unauthorized re-installation of software or utilities after removal also may result in a separate disciplinary action.

All Internet data that is composed, transmitted and/or received by City computer systems is considered to belong to City and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

The equipment, services and technology used to access the Internet are the property of the City and the City reserves the right to monitor Internet traffic and monitor and access data that is composed, sent, or received through its online connections.

All sites and downloads may be monitored and/or blocked by the City if they are deemed to be harmful and/or not productive to business.

Social Media:

The City of Pittsburgh has a tentative Social Media Policy. In the interim the following requirements should be followed at the very least:

- Do not let personal use of Facebook, Twitter, or other social networking sites interfere with work.
- Employees must get City approval to use social networking to conduct business.
- Any use of the City's name, seal, logo, or other intellectual property must be approved.
- Tweets may not disclose confidential or proprietary information.
- Employees should use common sense about what they post.