



Legislation Details (With Text)

File #: 2009-1873 **Version:** 2

Type: Ordinance **Status:** Passed Finally

File created: 10/20/2009 **In control:** Committee on Finance and Law

On agenda: **Final action:** 11/9/2009

Enactment date: 11/9/2009 **Enactment #:** 30

Effective date: 11/18/2009

Title: Ordinance amending and supplementing the Pittsburgh Code, Title Six: Conduct, by adding a new Article IX, entitled Privacy Policy for City Email and Data Systems.

Sponsors: William Peduto

Indexes: PGH. CODE ORDINANCES TITLE 06 - CONDUCT

Code sections:

Attachments: 1. 2009-1873.doc, 2. 2009-1873 Version 2.doc

Date	Ver.	Action By	Action	Result
11/19/2009	2	Mayor	Returned Unsigned	
11/9/2009	2	City Council	Passed Finally	Pass
11/5/2009	2	Committee on Finance and Law	Affirmatively Recommended as Amended	Pass
11/5/2009	2	Committee on Finance and Law	AMENDED BY SUBSTITUTE	Pass
10/28/2009	1	Committee on Finance and Law	Held in Committee	Pass
10/20/2009	1	City Council	Read and referred	

Ordinance amending and supplementing the Pittsburgh Code, Title Six: Conduct, by adding a new Article IX, entitled **Privacy Policy for City Email and Data Systems**.

WHEREAS: It is a well established principle that an employer owns all workplace computers and computer systems, and may access an employee's email and data files at will; and

WHEREAS: The City of Pittsburgh nevertheless wishes to place reasonable and ethical constraints on the City's power to access employee emails and data files; and

WHEREAS: The City of Pittsburgh seeks to preserve the integrity and independence of its separate branches of government; and

WHEREAS: These goals can be accomplished in a manner that protects the employee from unwarranted intrusion and promotes the City's interest in the appropriate and professional use of its computer resources; and

WHEREAS: These goals can be accomplished in a manner that is consistent with goals of government transparency and access to records;

Be it resolved by the Council of the City of Pittsburgh as follows:

Section 1. *Title Six: Conduct* of the Pittsburgh Code of Ordinances is amended and supplemented by the addition of a new *Article IX: Privacy Policy for City Email and Data Systems* as follows:

TITLE SIX: CONDUCT

ARTICLE IX:

Privacy Policy For City Email and Data Systems

CHAPTER 690: GENERAL PROVISIONS

§690.01 Definitions

Data File: A computer file which stores data or text for use by a computer application, system or user. For the purposes of this Article, Data Files include, but are not limited to, documents, spreadsheets and databases.

Email: a message sent from one individual to another individual or individuals via telecommunications links between computers or terminals.

Requester: For this purposes of this Article, a Requester is a Department Director presently employed by the City of Pittsburgh. For the purpose of this Article, the Office of Municipal Investigations shall be considered a City Department.

§690.02 Purpose

- (a) To limit access to by one City employee to another City employee's email and/or data files to situations involving a legitimate request submitted by a Department Director;
- (b) To be used in correlation with the City of Pittsburgh Electronic Communications Policy;
- (c) To maintain employee integrity and responsibility with minimal impact upon employee privacy;
- (d) To establish a definition of a legitimate request to view e-mail or data files.
- (e) To govern the internal access of City email and data files by another City employee. This policy is not intended to govern external requests for computer records, including but not limited to District Attorney requests, search warrants, grand jury subpoenas and court subpoenas generally, and Right to Know requests.

§690.03 System Maintenance

- (a) The Department of City Information Systems is charged with protecting City computer systems from outside intrusion and attack. CIS is also charged with protecting the integrity and privacy of internal user accounts.
- (b) Notwithstanding the terms of this Chapter, the Department of City Information Systems may enter a City of Pittsburgh employee's profile containing both emails and data files without completion of the following procedures, for the purpose of maintaining and supporting City computer systems.
- (c) The main objective for CIS interaction is network performance and not employee scrutiny.
- (d) Employee information shall not be intentionally viewed by CIS in the course of ordinary maintenance, unless a violation of the Electronic Communication Policy, City Code, or State law is evident.
- (e) Any information found to be non-job related is subject to deletion and/or authoritative notification.

CHAPTER 691: Procedures

§691.01 Procedures

The following procedures set forth a sequence of steps which a Requester must go through in order to obtain access to the email or data files of a City employee. Approval must be acquired at each consecutive stage

before advancement to the next stage.

- (a) Initial Request-The supervisor or manager of the Requesting Department must complete *Part I: Information Being Requested* of the *Permission to View Email and/or Data Files* Form, and forward to Department Director for approval.
 - i. The Initial Request must define the records sought with sufficient specificity as to subject matter, time frame and any other relevant criteria. Overbroad requests, or fishing expeditions, will not be entertained.
 - ii. If the Director deems the request to be valid, he/she will complete and sign the copy of the request and forward it to the Law Department for review and approval by the City Solicitor.
 - iii. If the Director denies the supervisor's request, the request will still be forwarded to the Law Department for final review.
- (b) Law Department: The Law Department will review both the Supervisor and Director's comments and recommendations in order to concur with the legitimacy of a request.
 - i. With the Solicitor's approval, the request will be forwarded to City Information Systems (CIS).
 - ii. Without the approval of the City Solicitor the request is fully denied and cannot proceed any further. There is no right of appeal from the Solicitor's denial of a request.
- (c) City Information Systems (CIS): The approved request will be forwarded to the Director of CIS to confirm whether the information is available and accessible.
 - i. The request will be assigned to a CIS network manager, who will search to determine whether the requested information is obtainable.
 - ii. If the information is found to be accessible, the assigned network manager will notify the Department Director and the City Solicitor, and will schedule a meeting for the purpose of viewing the information at the offices of City Information Systems.
 - iii. If the information cannot be accessed, the request will be deemed inconclusive and the Department Director and Solicitor will be notified that the request cannot be satisfied.
- (d) Viewing
 - i. The Department Director and the City Solicitor or their designees are the only approved personnel permitted to view any information approved for access.
 - ii. A designated time period will be assigned, according to the Department Director and City Solicitor, for access to the requested information.
 - iii. Viewing of information must take place within the offices of City Information Systems.
 - iv. At no time will information be sent / transferred to either the Department Director or City Solicitor's computer or hard drive for viewing.
- (e) Extra Information
 - i. The search of an employee's electronic data shall be limited to the information listed in the request form. It shall not be used as a way to search through all employee records. If any evidence of criminal activity is discovered during a search, that evidence shall immediately be reported to the appropriate authorities.
- (f) Notification
 - i. Within seven (7) days of the viewing of an employee's data, the City Solicitor shall submit written notice to the employee of the action taken, subject to the following exceptions:
 - A. Where the wrongful behavior alleged in the request for e-mails would constitute a violation of federal or state law, no notification will be required until any criminal investigation is complete;
 - B. No notification is required when the information is requested pursuant to a grand jury subpoena or any other court subpoena;
 - C. No notification is required when the information is viewed pursuant to a right to

know request unless e-mails are found to be public records and released to the requester;

- D. In the case of investigations initiated by OMI, the Director of OMI may request that the Solicitor grant an exemption from these notification requirements. The Solicitor and the Director of OMI will maintain a log of all such requests;
- E. If the information is viewed as part of an Ethics Hearing Board investigation, the parties will be notified at the conclusion of the investigation;
- F. No notification is required when the author of the email or data file is no longer employed by the City of Pittsburgh;
- G. The City Solicitor may grant an exemption from the notification requirement in any circumstance where notification would violate a City or State law, or any court imposed privilege, or compromises the rights of the City in any litigation.

(g) Records

- i. The Law Department shall maintain a copy of all request forms regardless of whether the request is approved or denied.

§691.02 Retention of Information

- (a) Any duplication of emails or data files is limited to hard paper copies only, and must be pre-approved on the request form through the Law department.
- (b) Information that is duplicated, will be gathered and sent back to Department Director following the meeting, and review of information by the Law Department.
- (c) No duplicates may be gathered through soft-copy devices or source. No flash drives, cameras, or any other form of electronic device that is capable of retaining information is permitted into the viewing.
- (d) Information to be duplicated must be identified immediately after the viewing.
- (e) The City Solicitor may waive the requirements of this section where the transfer of soft copy documents will advance City interests, such as when the work product and email files of a former employee are accessed in order to complete a project or task.

CHAPTER 692: Special Procedures

§692.01 Special Procedures

(a) City Clerk Staff

- i. For the purposes of this Chapter, the President of City Council shall be considered the Director for an employee of the City Clerk's office.

(b) City Council Staff

- i. For the purposes of this Chapter, the Council Member shall be considered the Director for any employee in his/her office.

(c) Elected Official

- i. If there is a need to review the electronic files of the Mayor, City Controller, or a Member of City Council, the request must be approved by the City Solicitor, the Director of CIS, and the Chair of the Ethics Hearing Board.

(d) Solicitor

- i. If there is a need to review the electronic files of the City Solicitor, then the request must be approved by the Mayor, the Director of CIS, and the Chair of the Ethics Hearing Board.

(e) Director of CIS

- i. If there is a need to review the electronic files of the Director of CIS, then the request must be approved by the Mayor, the City Solicitor, and the Chair of the Ethics Hearing Board.

CHAPTER 693: Penalties

§693.01 Penalties

The following violations are subject to penalties under this section:

- (a) An attempt is made to gain access without a completed and approved request form.
- (b) Information is distributed by City Information Systems without signatures of both the Department Director and the City Solicitor.
- (c) Information is retained and duplicated without proper approval from the Law Department on request form.
- (d) Unapproved and unrequested employee information is acquired during "system maintenance".
- (e) Any Violator is subject to administrative discipline up to and including termination.
- (f) Notification of violation of this Article shall be made to the District Attorney.

Permission to View Email and/or Data Files Form

Part1: Information being requested

Employee's Name:

Employee's Department:

Requested Electronic Information: Email(s)	Data File(s)	Both
--	--------------	------

Reason for Request:

Hardcopies requested if legitimate information is found:	Yes	No
--	-----	----

Supervisor Signature	Date
----------------------	------

Part 2: Department Director	Date Received:
-----------------------------	----------------

This request is:	Approved	Disapproved
------------------	----------	-------------

The Reason(s) for Request Approval/Disapproval:

Department Director Signature	Date
-------------------------------	------

Part 3: Law Department	Date Received:
------------------------	----------------

