

Developing Sensible E-mail and Internet Use Policies

Sands L. Stiefer

Sands L. Stiefer is chief deputy, Harris County Appraisal District, Houston, Texas.

The statements made or views expressed by authors in Assessment Journal do not necessarily represent a policy position of the International Association of Assessing Officers.

Introduction

At the Harris County Appraisal District, we have had internal e-mail for about eight years, Internet e-mail and web access for about six years. We have just begun using workflow software, a cross between e-mail and an assembly line. In many cases, these tools have revolutionized the way we do business, both internally and externally. There is no question that eventually they will affect every area of the state and every person in it. However, there are some grim realities that employers must face when working with this brave new technology. First, we have to ask: How can we ensure that employees use electronic media in the way we intend when we make it available? Consider the following:

- A survey of 1,000 human resources managers by the American Management Association revealed that 31 percent of those managers had received reports of employees' receiving sexually harassing e-mail at work.
- One survey indicates that Internet users spend about 70 percent more time at work visiting financial sites (for example, tracking stocks) than they do at home.
- Large companies are beginning to use software designed specifically to block employees from sending sexually harassing e-mail.
- One Tennessee court has already considered lewd e-mail, together with unwanted physical contact, as sufficient basis to support a sexual harassment judgment; Chevron recently paid \$2.2 million to settle claims of e-mail sexual harassment.

E-mail harassment is particularly problematic because it can be done privately (unless an agency monitors e-mail, it won't know that it is happening), and even if the e-mail is later deleted, it often remains somewhere in the system and may be used against the employer later. The problem isn't limited to sexual harassment: suppose you have an employee who decides to send hostile e-mail to the city council, the local newspaper, or the IRS using your agency's e-mail address. Is the communication from the employee or from you? Public agencies face an additional problem in that e-mail may be subject to disclosure under public information and open records laws. Similarly, web use is generally private, but just as e-mail may endure long after it is deleted from a user's system, records of web use and misuse may endure in cache files, firewall records, or cookies, or on some web server or other computer. On the other hand, in the absence of clear policies, employees may devel-

op reasonable expectations of privacy, and it is theoretically possible to put yourself in such a position that you can't discipline employees without violating their legal rights. Most advice on this subject boils down to the following points:

- If you provide Internet access and/or e-mail, develop a policy for its use.
- Distribute the policy in writing to every employee. Ideally, get a signed receipt from each employee that the policy is understood.
- Don't go overboard, reading every e-mail or visiting every website an employee has visited, unless you have reasonable grounds to believe that misuse has taken place. Be very specific about prohibiting visits to pornographic sites or sites that display information that could be construed by others as contributing to a hostile environment.

Developing a Policy

Some points to consider in drafting a policy:

Scope of Policy

How far-reaching will the policy be? Suppose, for example, that you allow employees to access your agency's Internet account or their e-mail accounts from home. Will the policy apply only to use on agency premises? Will it only apply when agency equipment is being used? Will it apply anytime employees send or receive mail through their agency Internet accounts? If employees have their own personal e-mail accounts, may they use agency equipment, time, or media to access them?

Ownership of E-mail

Who owns the e-mail that employees write? Is all e-mail considered official correspondence from the agency? If not, should their signature blocks carry some disclaimer?

Privacy and Monitoring

What will the policy be on privacy of e-mail correspondence and records of Internet use? To what extent will employees be monitored? (See figure 1 for a sample policy.)

Passwords

Will employees have the authority to set or change their own passwords? If so, must they provide your agency with lists of the passwords for their machines?

Use for Personal Communications

May employees send or receive personal e-mail? May they shop online? Conduct businesses on the side? May they use their own web-based e-mail accounts in addition to the agency account(s)? If the capability is available, may employees monitor their personal e-mail accounts using agency equipment or software?

Responding to Outside E-mail

Who will be responsible for answering e-mail received from property owners? To whom should messages be forwarded? (See figure 2 for a sample policy.)

Offensive or Improper Messages

Will sending and/or receiving offensive or improper messages be prohibited? What is considered offensive or inappropriate?

Signature

Will there be any restrictions on how employees' signature blocks should read? Must employees always identify themselves in the body of each message?

Appropriateness of E-mail v. Other Media

Assuming employees have legitimate purposes, when should they use e-mail in place of ordinary memoranda, letters, or telephone calls? How long and in what form should such "official" e-mail messages be retained?

Confidential and Sensitive Information

Will employees be permitted to send confidential or sensitive information by e-mail?

Internet E-mail v. Internal E-mail

If the agency has both, what purposes should be assigned to each?

Mailing Lists and Receipt of Personal E-mail

May employees subscribe to Internet mailing lists or to services that deliver personalized e-mail? if so, must they be business-related?

Examples of Acceptable and Unacceptable Uses

Give examples of what you consider to be permissible or acceptable uses and what you consider to be unacceptable uses. (See figure 3 for a sample policy.)

Checking E-mail

How often must employees check e-mail? Who is responsible for checking e-mail if an employee will be out of the office for an extended period?

Acceptable/Unacceptable Website Visits

Provide examples of acceptable and unacceptable types of websites.

Downloading Software and Other Files

May employees download software or other files from the Internet? May they send/receive files by mail or FTP?

Virus Protection

Must employees use virus protection software?

Record Retention

How long must employees keep e-mail received from outside? How long must responses be kept? How will e-mail be archived if it needs to be kept for a long time?

Public Information Requests

Note that many e-mail messages are subject to disclosure under public information and/or open records laws.

Figure 1: Privacy and Monitoring

2.3 Electronic information created and/or communicated by an employee using e-mail, word processing, utility programs, spreadsheets, voice-mail, telephones, Internet/BBS access, etc., will not generally be monitored by the company, and we respect our employees' wish to work without "Big Brother" looking over their shoulder. However, the following conditions should be noted:

2.3.1 The company routinely monitors usage patterns for both voice and data communications (e.g., number called or site accessed; call length; times of day calls). Reasons include cost analysis/allocation and the management of our gateway to the Internet.

2.3.2 The company also reserves the right, in its discretion, to review any employee's electronic files and messages and usage to the extent necessary to ensure that electronic media and services are being used in compliance with the law and with this and other company policies.

2.3.3 Employees should therefore not assume electronic communications are totally private and confidential and should transmit highly sensitive information in other ways.

From Adam Conti, Sample Employer E-mail and Electronic Usage Policy, Available from www.conti-law.com/EmailNo2.html.

Figure 2: Responding to Outside E-mail

D. Accessing E-mail

1. E-mail is used for official communication and staff members must check their e-mail weekly. Staff with increased responsibility levels should check more frequently or as directed by their supervisor/manager. Staff are responsible for reading all information in official communications distributed electronically.

2. Electronic receipts may be used to verify that employees have received certain messages, When Administration sends out a message of special importance, for example, regarding policies and procedures, the sender may use an option that alerts him/her when each recipient has opened the message....

E. Responding to E-mail from patrons

Type of Communication	Appropriate Response
Reference request	answered by the department manager questions treated as a telephone "call back" for-ward question/response to the appropriate library manager (NWL or OWL) for use in assessing impact of cyber requests on staff time/public service
Compliment	forward to the NWL/OWL library manager
Complaint	forward to the NWL/OWL library manager
Policy question or challenge	forward to the NWL/OWL library manager

Harassing/offensive message	forward to the NWL/OWL library manager
Commercial notice from vendor	handle like printed notices if quantity becomes unwieldy from particular vendor, alert Technology Coordinator
Request for change to web site	forward to the Technology Coordinator

1. Patrons can direct comments to administrators, managers and designated staff from the Worthington Public Library's Web Site. There are various types of transmissions that might be received. These guidelines should be followed in responding to e-mail from patrons.

From Worthington Public Library, Email [sic], Staff Use (Worthington, Ohio, 1998). Available from winslo.state.oh.us/publib/woplemai.html.

Figure 3: Examples of Acceptable and Unacceptable Uses

Section IV: Personal Use of Internet

a. Internet access is intended for official County business. Abuse of Internet access includes but is not limited to the following:

1. engaging in any unlawful or malicious activity;
2. misrepresenting a personal communication as an official communication;
3. sending a chain letter;
4. sending, receiving, or accessing pornographic materials;
5. using objectionable language;
6. advertising personal items.

b. Proper use of Internet access includes the following:

1. downloading job-related information;
2. sending and receiving job-related e-mail messages and file attachments;
3. making business arrangements;
4. searching job-related databases;
5. using the Internet for occasional, brief personal communications, where those do not violate any other provisions of this section or, in the view of officials and department heads, do not interfere with County business.

From Williamson County, Electronic Systems Use Policy

(Georgetown, Texas, 2000), 2.

*Developing Sensible E-mail and Internet Use Policies, by Sands L. Stiefer, Assessment Journal, March/April 2000, p. 53-55.
Reprinted with permission of the International Association of Assessing Officers, 130 East Randolph, Suite 850, Chicago, IL 60601;
www.iaao.org.*