

Published by the  
Glatfelter Insurance Group  
York, Pennsylvania

# Employment Practices UPDATE

## The “Smoking Gun” in Employment Litigation:

*Email and Internet Communications*



**An inherent problem with emails involves the perception that formal standards of conduct or ethics are lessened because of the informal method of communication.**

We welcome comments, suggestions and questions from our readers.

Write to:  
Editor  
Employment Practices Update  
P.O. Box 2726  
York, PA 17405

epupdate.opinion@vfis.com



A group of women sued their employer for sexual harassment, alleging the organization permitted its internal email system to be used for transmitting sexually offensive messages. In accusing the organization of allowing a hostile work environment, the women pointed to a “smoking gun,” an email message that circulated throughout the organization titled, “25 Reasons Why Beer is Better than Women”. This electronic “smoking gun” evidence is part of the reason the company, Chevron, paid \$2.2 million to settle the sexual harassment lawsuit.

At a time when emails and other technology communications pose tremendous risk, many emergency services organizations (ESOs) are taking little action to reduce the risk. This article explores risk management measures your ESO can take to prevent misuse of email and Internet systems and prevent security breaches.

The law is clear that an ESO is required to make reasonable efforts to prevent workplace harassment and discrimination. In the current hyper-litigious society, your ESO can gain substantial legal protection by proactively working to reduce the threat of inappropriate email and Internet usage. Specifically, your ESO should consider the following risk management measures:

1. Develop a comprehensive electronic communications systems policy.
2. Train employees and volunteers (members) on the policy and have them sign a form acknowledging their understanding of the policy and internal reporting processes should there be a policy violation.

3. Implement technical safeguards such as computer filtering systems and security protection.

### **Inherent Risks with Email**

In the last 10 years, email has become, for many, the preferred means of professional and personal communication. Benefits of email include its ease of use, speedy delivery, ability to send attachments and reach multiple recipients, and widespread accessibility on computers or handheld devices. So why does email present such a risk to ESOs?

**Informal communications** — An inherent problem with email involves the perception that formal standards of conduct or ethics are lessened because of the informal method of communication. An ESO member would certainly not include offensive statements or photographs in a memorandum addressed to members of the ESO Board of Directors or Commissioners. Somehow, standards of decorum are tossed out the window when email is the chosen means of communication. The truth is that content found in an email message or as its attached document, photograph, video, or cartoon is just as susceptible to discovery in litigation as formal correspondence.

People often use email to express opinions and emotions that they typically would never declare in a conventional written document. For instance, when completing a formal counseling form or performance evaluation, supervisors are careful not to inject subjective views, speculation, or superfluous information. However, in a less formal setting as when writing an email message, supervisors often let their guard down and include commentary and opinions that are irrelevant to the subordinate’s performance or behavior.

Another potential pitfall associated with email usage involves spreading rumors or gossip. Again, the informal nature of emails leads to promulgating inflammatory gossip not intended for the public’s eyes. Regardless of intent, sensational email correspondence may be used as evidence in a harassment, discrimination, or wrongful termination lawsuit.

*Continued on page 2*

## The “Smoking Gun” in Employment Litigation: Email and Internet Communications

Continued from page 1

**Ease of forwarding** - How many times have you received an inappropriate joke, picture or video that was forwarded via email? The number is probably too high to count. Now be honest, how many times have you forwarded the same email to a coworker or person outside of the ESO?

You may not be the original author of the joke or email, but forwarding to others gives you ownership of the content. Forwarding the message conveys perceived acceptance of the email's subject matter. Passing on the email is much like the end of a political television commercial when the candidate states, “My name is Bob Jones, and I approve of this message.”

In hostile work environment litigation, an ESO member's email history may be tracked, revealing a propensity to forward inappropriate jokes or attachments (pictures, videos, drawings, or links to websites). The ESO member may attempt to defend himself by saying, “Those weren't my words in the jokes or emails. I just passed them on, not intending any harm to anyone by sending them.” In the end, the content of the email is sent with your name at the top of the document, much like letterhead. So, your name may be associated with the message, whether the content is sexually insensitive or insulting to someone's gender, race, color, national origin, religion, or disability.

**Lack of control** - Although the ease with which email may be forwarded make it an efficient communication tool, it also poses significant risks. When an email message is sent to someone, you have no control over whether that person keeps your message confidential or circulates it to any number of other people. It is possible for the content of the email to be posted on the Internet, where it may be viewed by countless persons outside of your ESO. This is a particular concern if your message contains sensitive employment-related information, such as commentary about a member's performance or an internal investigation.

**Does “deleted” mean the email is gone forever?** The answer is most likely “no”.



**Content found in an email message or its attachment is just as susceptible to discovery in litigation as formal correspondence.**

The ability to retrieve what is believed to be a deleted email is another reason email usage can pose a serious risk to your ESO. Computer professionals can utilize widely available software and expertise to find messages that have been deleted for some time. Often backup copies of emails exist on the sender's or recipient's computer or on the ESO's network. Also, if an email is sent through a commercial service (e.g., AOL) or over the Internet (e.g., Yahoo or Hotmail), the email likely passed through several computer systems before reaching its final destination. Each computer in the chain between sender and recipient normally retains a copy of the email message.

### Policy Development and Dissemination

With the assistance of local labor and employment counsel, your ESO should develop a comprehensive Electronic Communication Systems (ECS) policy. Consider the following key issues for inclusion:

1. Prohibit inappropriate transmittal or downloading of material that is harassing, discriminatory, offensive, pornographic, defamatory, or otherwise inappropriate.
2. Prohibit copying or sending confidential information.
3. Inform members that:
  - they should not expect that their communications through and use of the ESO's computer systems are confidential or private; personal privacy interests are limited while conducting ESO business, on ESO property, or while using ESO-owned equipment.

- the ESO reserves the right, with or without notice, to access, monitor, review, copy, and/or delete any computer files, emails sent or received, and all Internet communications or transactions.

- Any violation of policy numbers 1 and 2 will result in discipline, up to and including discharge.

Periodic education and training for all ESO members is necessary in many areas, and this is no exception. Members should sign an acknowledgement form indicating their receipt and understanding of your ECS policy as well as their agreement to report known or suspected policy violations.

### Technical Safeguards

It is nearly impossible to enforce an Electronic Communications Systems policy without implementing software that monitors email and Internet usage. For instance, computer filtering software can flag messages containing offensive, discriminatory, or suspicious words. Consider installing an on-screen display of your policy that appears every time members log onto their computers. Remember, technology safeguards can help prevent incidents of harassment, malicious gossip, and dissemination of confidential information.

### Conclusion

Using technology to filter email and review use of any Internet communications can demonstrate that your ESO has taken reasonable measures to prevent incidents of harassment, discrimination, defamation, or confidentiality leaks. If an incident of wrongdoing occurs or inappropriate materials somehow slip through the cracks, your earlier implementation of a detailed Electronic Communication Systems policy, backed up by training and technology enforcement, provides an important component of a legal defense against a hostile work environment claim.

*Michael McCall, J.D., provides employment practices consulting and training to emergency service organizations nationwide.*

### Employment Practices UPDATE

Photocopying or transferring this document is a violation of federal copyright law and is prohibited without the express written consent of VFIS. VFIS does not offer legal advice. Readers should seek the advice of an employment attorney regarding any legal questions.