Compliance Building

Doug Cornelius on Compliance and Business Ethics

Compliance Policies and Email

Posted on Thursday, April 2nd, 2009 at 7:00 am.

You should take a look at your computer use and email policies to see how they address three recent cases involving email in the workplace.

The first case involves unauthorized acces: (*Van Alstyne v. Electronic Scriptorium, Inc.*). The president of the company had broken into an employee's personal AOL email account. The employee had occasionally used that email account for business communications. To top off the bad behavior, the president of the company had propositioned the employee before firing her and then accessing that email account.

In the second case (*Stengart v. Loving Care [.pdf]*), Ms. Stengart resigned from Loving Care and sued the company. Before leaving she e-mailed her lawyer through her personal web-based account from her company-issued computer using the company's internet access. Loving Care recovered temporary files stored on that computer which contained copies of Stengart's attorney-client communications. Stengart discovered that Loving Care's lawyers planned to use her e-mail in the litigation. She asked the trial court to decide whether the e-mail, sent during work hours on a company computer, was protected by the attorney-client privilege. The court held that it was not.

In the third case (*Noonan v. Staples*), Staples fired sales director Alan S. Noonan for padding his expense report. Executive Vice President Jay Baitler sent an e-mail to approximately 1,500 employees explaining the reason for the firing. The e-mail contained no untruths, but Mr. Noonan sued for defamation anyhow. Unfortunately for Staples, truth is not a defense in Massachusetts if the challenged statement was communicated with actual malice.

Lessons? What should you have in your company's computer policy?

First, tell employees that they should not use personal e-mail accounts for purposes of conducting company business.

Second, the company should have a policy that any message sent from a company computer is subject to disclosure and the employees should not have an expectation of privacy.

Third, employees should not access another employee's files or email accounts, whether they are the company's or personal.

Fourth, employees should not use email or company computers to send malicious messages.

Finally, make sure you can prove that each employee knows these rules.

See:

- Web-Based E-mail Accounts Accessed At Work: Private Or Not? Look To The Handbook from Workplace Privacy Counsel
- E-Mail Dangers for Employers by Frank Steinberg of the New Jersey Employment Law Blog
- *Stengart v. Loving Care (pdf)*
- Van Alstyne v. Electronic Scriptorium, Inc. hosted by JD Supra
- How Not To Fire Someone for Workplace Fraud – previous post on *Noonan v. Staples*