

Full Speed Ahead: Managing Technology Risk

Resource Type: Risk eNews

Topic: Data Privacy, Tech Risk, Cybersecurity, HR Risk and Employment Practices

Preventing Employee Misuse of Technology

A nonprofit employer places a great deal of trust in its employees when providing equipment and an electronic connection to the outside world. The survival and viability of your nonprofit may depend on how, and whether, employees uphold that trust, and how well you educate them about your expectations and train them in the proper way to use the equipment. The rule-of-thumb is “Don’t assume.” The codicil is “Don’t deny,” because the Internet and e-mail are very effective and efficient tools for managing the business of your nonprofit when used appropriately. In your zest to reduce the risks associated with Internet use, don’t cavalierly deny employees access to this modern tool.

Every nonprofit can and should take steps to both educate its workforce about its role and responsibility to protect the organization’s technological assets, and the organization’s specific expectations with respect to employee use of equipment and systems. Never assume that employees “know better.” Whether you’re prohibiting visits to pornographic Web sites or restricting the downloading of freeware from the Internet, sound risk management requires that you provide explicit instructions about your expectations at the outset of the employment relationship. Provide reminders about acceptable use from time to time, as appropriate. Update your policies as new technology risks emerge. The admonition “Don’t open an attachment to an e-mail from someone you don’t know” is commonly heard risk management advice today. Like other suggestions contained in *Full Speed Ahead: Managing Technology Risk in the Nonprofit World*, this advice was born from real world experience — in this case from destructive viruses transmitted through enticing e-mail messages. As with any employment-related policies, the effectiveness of a technology policy is seriously compromised if the organization establishes — but ignores — the policies it adopts.

Risk Management Steps to Guard Against Employee Misuse of Technology

- Provide explicit instructions about the organization’s expectations with respect to employee use of technology.
- Provide periodic reminders about acceptable and unacceptable uses of the organization’s systems.
- Require that employees sign a copy of the organization’s technology or acceptable-use policy and keep a copy of these signed documents in each employee’s personnel file.
- Be aware that new uses of technology may need to be prohibited; thus aspects of your policies may require periodic updating.
- Don’t let the organization’s acceptable-use or technology policy gather dust. Review them frequently and change the policies as needed.
- Apply use restrictions evenly in your organization.

These risk management steps were taken from *Full Speed Ahead: Managing Technology Risk in the Nonprofit World*, Chapter 2, “Preventing Employee Misuse of Technology,” pages 11-12.

The Nonprofit Risk Management Center welcomes questions and comments at 703.777.3504.