CALIFORNIA RURAL WATER ASSOCIATION
MEMBERGUARD
Serviced by Glatfelter Public Practice

RISK COMMUNIQUÉ

A technical reference bulletin by the Risk Control Services Department of the Glatfelter Insurance Group

Electronic Communication Systems (Internet & E-mail Usage) – Risk Management for Management Liability & Employment Practices

Technological advancements have dramatically heightened the risk of personnel-related litigation for organizations. The increased accessibility of computers, Internet, e-mail, television and cell phones raises the number of costly lawsuits facing organizations. Hostile work environment claims often involve elements of technology, such as inappropriate e-mail messages or Internet usage. Moreover, organizations frequently are forced to address their employees' inappropriate utilization of technology, resulting in discipline such as suspension, demotion and termination.

This Risk Communiqué offers risk management guidelines for addressing electronic communication systems within your organization. The goal is to assist your organization in preventing technology abuses and reducing your exposure to personnel-related claims.

Developing and Implementing a Policy and Procedure

Organizations are under a duty to implement written policies and procedures designed to provide a workplace free from harassment and discrimination, as well as to prevent confidentiality breaches. It is prudent risk management to develop or update an organization's policy governing all electronic communications, not just Internet and e-mail usage. Organizations face increasing risks with other forms of technology, such as personal cell phones (i.e., inappropriate pictures taken with these phones) and television viewing (i.e., displaying pornographic or other sexual content on organization property).

Employees should receive and sign a form acknowledging their understanding of the parameters of the electronic communication systems policy and the organization's ability to monitor their usage. It is recommended that organizations retain legal counsel specializing in employment and labor law to review and approve policy language prior to implementation.

Preventing Harassment and Discrimination

Employees more willingly accept restrictions on their usage of electronic communication systems when organizations integrate them with existing non-discrimination and harassment policies. Organizations must clearly communicate that electronic communication systems are not to be used in any way that may be disruptive, offensive to others, or harmful to morale. The organization policy should prohibit the display or transmission of sexually explicit pictures, messages, videos, or any transmission or use of communications that contain profane or offensive language, ethnic slurs, racial epithets, or anything that may be construed as harassment, discrimination, or disparagement of others based on race, color, national origin, gender, age, disability, religion, sexual orientation, or political beliefs. Additionally, computer software programs may also be purchased to help filter inappropriate subject matter.

Organization's Right to Monitor

Most national studies and surveys conclude that approximately seven of ten American workers access the Internet at work for non-work purposes and that more than one-half send and receive personal messages on their work e-mail accounts.

This is a sample guideline furnished to you by MemberGuard. Your organization should review it and make the necessary modifications to meet the needs of your organization. The intent of this guideline is to assist you in reducing risk exposure to the public, personnel and property. For additional information on this topic, you may contact your Risk Control Representative. www.MyMemberGuard.com

Granting employees access to electronic communication systems while on the job is a privilege and not a guaranteed personal right. Availability of technology on the job is designed to enhance business practices, rather than decrease productivity and increase legal liability for the organization. While employees have a reasonable expectation of personal privacy at work, organizations must communicate that these privacy interests are limited while conducting organization business, on organization property, or using organization-owned equipment.

Policies should indicate that all computer files, including e-mails sent or received, are considered and treated as if they are business-related information. They should also reflect that the organization not only has the capability, but reserves the right, with or without notice, to access, monitor, review, copy, and/or delete any computer files, including e-mail sent or received, and all web site communications and/or transactions.

Technology Filters and Safeguards

Monitoring software is essential for preventing employee access to inappropriate Internet sites and curbing e-mail abuses. Computer filtering software can flag messages containing offensive, discriminatory, or suspicious words. Organizations should consider installing an on-screen display of the electronic communication systems policy that would appear each time employees log onto their computers. Such technology safeguards can help remind employees that their usage is monitored, and prevent incidents of harassment, malicious gossip, and dissemination of confidential information.

Discipline

Many organizations are being forced to discipline employees for abusing electronic communication systems. Penalties for those who violate organization policy and engage in harassing, discriminatory or other inappropriate behavior typically would follow a progressive disciplinary process. However, in some circumstances, a first violation may be severe enough that termination may be the most appropriate finding. For example, accessing pornography is the most common prohibited computer activity that leads to disciplinary action. Policies should set forth the organization's right to determine and administer harsh and consistent discipline for those violating harassment, discrimination, or confidentiality standards.

This is a sample guideline furnished to you by MemberGuard. Your organization should review it and make the necessary modifications to meet the needs of your organization. The intent of this guideline is to assist you in reducing risk exposure to the public, personnel and property. For additional information on this topic, you may contact your Risk Control Representative. www.MyMemberGuard.com