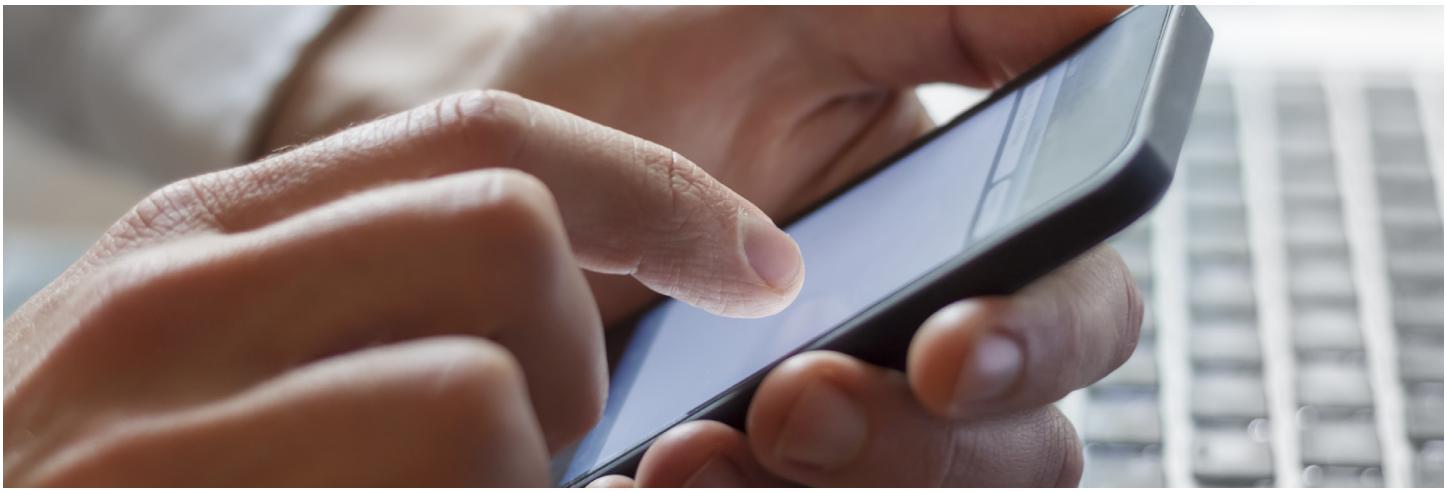
ELECTRONIC COMMUNICATION SYSTEMS (INTERNET & E-MAIL USAGE) –

RISK MANAGEMENT FOR MANAGEMENT LIABILITY & EMPLOYMENT PRACTICES



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

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

DEVELOPING AND IMPLEMENTING A POLICY AND PROCEDURE

Community care organizations, like other companies, 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 your organization's policy governing all electronic communications, not just Internet and e-mail usage. Employers 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 company property).

Employees should also 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 PREVENTION

Employees more willingly accept restrictions on their usage of electronic communication systems when organizations integrate them with existing non-discrimination and harassment policies. Policies should 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. 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. It should also prohibit any communication 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.

EMPLOYER'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 email accounts.

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, the organization must communicate that these privacy interests are limited while conducting business, on company property, or using company-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 member access to inappropriate Internet sites and curbing e-mail abuses. Computer filtering software can flag messages containing offensive, discriminatory, or suspicious words. Consider installing an on-screen display of the organization's electronic communications systems policy that would appear each time members log onto their computers. Such technology safeguards can help remind members that their usage is monitored, and prevent incidents of harassment, malicious gossip, and dissemination of confidential information.

DISCIPLINE

More organizations are being forced to discipline employees and volunteers for abusing electronic communication systems. Penalties for those who violate 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.

SUMMARY

Distracted driving and risky behaviors behind the wheel contribute to countless preventable accidents each year. Fleet managers have taken steps to help reduce the number of accidents. Today there are a number of technology-driven tools that may prove to be useful in avoiding a significant number of these accidents and may be worth investigating for your vehicle fleet.

©2012 Glatfelter Insurance Group | All Rights Reserved. The information and recommendations offered by Glatfelter Insurance Group herein and in related materials are provided solely for your consideration in risk control efforts. Glatfelter Insurance Group specifically disclaims any liability for any act or omission by any person or entity in connection with the preparation, use or implementation of plans, principles, concepts or information contained in this publication. The information contained in this publication is intended for educational purposes only and is not intended to replace expert advice in connection with the topics presented. The intent of this guideline is solely to assist you in reducing risk exposure to the public, personnel and property, and Glatfelter Insurance Group makes no warranty as to results. Your organization should review it and make the necessary modifications to meet the needs of your organization.

Design Updated 2026