

Instant Messaging & Camera Phones Increase Risk

Contributed by Victor O. Schinnerer & Company Inc.

August 2006

The AIA collects and disseminates Best Practices as a service to AIA members without endorsement or recommendation. Appropriate use of the information provided is the responsibility of the reader.

CONSULT YOUR ATTORNEY

The information herein should not be regarded as a substitute for legal advice. Readers are strongly advised to consult an attorney for advice regarding any matter related to this subject.

SUMMARY

The recent growth in the popularity of personal communication innovations—particularly instant messaging (IM) and camera phones—presents potential liability for employers. Camera phones and instant messaging are so new that many employee handbooks probably do not address them. However, it is important for an employer to understand the risks associated with these technologies.

INSTANT MESSAGING CAN CREATE INSTANT EXPOSURE

Most offices have policies that address Internet activities such as e-mail and downloading, but that is not enough. An effective office Internet-use policy must also cover instant messaging, which works like e-mail, only faster. It's a comment-by-comment form of e-mail where information is exchanged at real-time speeds.

Employees use IM to communicate with coworkers, business associates, friends, and relatives. Often, companies are unaware that IM is occurring at their offices and to what extent. Some experts estimate that as many as half of all employees nationwide use IM or similar software to communicate while at work.

The informal language often used in IM can convolute an intended message. Even if IM consistently conveyed the intended message, the activity still has the potential to create exposures. The most obvious negative impact associated with IM is the distraction from productive activities. A constant running thread of communication on an employee's monitor makes for poor time management.

On a more extreme level, the ease of communication can lead to violations of professional

and contractual confidentiality commitments. Instant messaging to client representatives can change expectations or create doubt about the quality of services. Casual, in-firm communication can even provide documented support of discrimination or harassment charges.

Firms that have not addressed the issue should develop an IM-use policy. The policy should address whether instant messaging is allowed and, if so, the scope of the communication, restrictions on content, and retention procedures.

CAMERA PHONES POSE UNIQUE PROBLEMS

With camera phones, employees can easily take digital photographs of a client's confidential information or copy their employer's protected records. In addition, the use of camera phones can easily lead to harassment or discrimination claims. Camera phones present potential risks that are exacerbated by the difficulty in monitoring and detecting the use of such phones.

A firm's best defense against the inappropriate use of camera phones is a clear policy regarding their use. While an employee handbook policy cannot eliminate the possibility of camera phone abuse, it can set guidelines and parameters, thereby limiting the opportunity for abuse. Some employers may ban camera phones altogether since they represent a threat to client confidentiality and the firm's operations.

POLICIES MUST BE UPDATED

Both of these technologies, if ignored by employers, can quickly lead to harassment or discrimination lawsuits, claims of breach of confidentiality, and challenges to firm security. While a policy could be written to include emerging technologies, it makes more sense to develop policies that are as specific as possible and are updated as needed. Policies should focus on the firm's concern for security, how the firm monitors employees' communications, and penalties for abuses.

POLICIES MUST BE ENFORCED

Any changes in policy must be communicated to all employees. Choose the most effective delivery method for your office, whether it is print or electronic circulation. Whichever method you choose, be sure to require employees to acknowledge they have read the message, either by clicking on a link or signing a document. Experts agree, however, that having a policy is pointless unless it is enforced. With IM and camera phone use, constant enforcement of a rational policy is essential to avoid claims from clients and employees.

RESOURCES

More Best Practices

The following AIA Best Practices provide additional information related to this topic

- 10.02.01 Electronic Data Transfer: A Guide To Managing Opportunities and Risks
- 10.02.06 Watch Your Language: The Risks of E-mail
- 13.03.06 Watch Your Language: The Risks of E-mail

For More Information on This Topic

See also "Using the Internet in Practice" by Paul Doherty, AIA, and Michael Tardif, Assoc. AIA, *The Architect's Handbook of Professional Practice*, 13th edition, Chapter 13, page 392.

See also the 14th edition of the *Handbook*, which can be ordered from the AIA Bookstore by calling 800-242-3837 (option 4) or by email at bookstore@aia.org



Feedback

The AIA welcomes member feedback on Best Practice articles. To provide feedback on this article, please contact: bestpractices@aia.org

Key Terms

- Practice
- Business planning
- Quality control programs
- Risk management



Two Wisconsin Circle
Chevy Chase, MD 20815-7022
(301) 951-9746
www.planetAEC.com

Portions of this Best Practice are a contribution of Victor O. Schinnerer & Company, program administrators of the AIA Commended Professional Liability Insurance Program.