THE NEWSLETTER FOR LEGAL OFFICE MANAGERS

LAW OFFICE ADMINISTRATOR™

Volume XX/ Number 3 MARCH 2011

A new risk firms need to address: social media

DANGERS UNTHOUGHT OF FOUR YEARS AGO

There's a grave new world out on the internet. It's social networking.

"It's only a few years old, yet it has turned the workplace upside down," says **RICHARD WEINBLATT, Ed.D.**, a/k/a The Cop Doc, an Orlando, FL, consultant to both employers and law enforcement on crime and safety issues. Weinblatt is also a former police chief.

Technology misuse is nothing new, he says, but what was seen previously is nothing to what is being seen today, mainly because of the "ease and immediacy and anonymity the internet provides."

On social sites, "people do downright criminal things" such as stalking and harassing coworkers or supervisors. Equally disturbing, the social sites have become the vehicle of choice for virus infiltration.

"It's new territory" that few employers have addressed.

Because of the risks – both seen and unforeseen – administrators need to set rules for social media use and enforce them with protective technology as well as disciplinary consequences. Social media is much like sexual harassment, he says. It's far-reaching to the point that it warrants its own separate policy.

NOT AN EASY THINGS TO BAN

Start with a yes or no. Can employees even go to the social websites during work hours?

The answer, Weinblatt says, isn't as simple as it seems. While banning the sites entirely might appear to be the safest approach, it's not practical, because there's no way to enforce it.

What's more, with social sites have become so popular that a ban can be souring. "Employees need a breather now and then, and it's not bad to spend a little time on Facebook or Twitter as long as they aren't accessing objectionable material."

He finds that the most acceptable and also most doable position is middle-of-the-road where the firm limits the time people can spend on the sites.

But be specific about it. Don't just say "excessive use" is not allowed. Set a timeframe for use, a reasonable amount being from 30 minutes to an hour a day.

FORBID THE UNEXPECTED

Along with that, set rules of conduct for the sites, and apply them to both in and outside the office.

Prohibit comments that are harassing, indecent, or disrespectful of the firm, its employees, or its clients.

Forbid discussion of client matters.

Forbid "unbecoming behavior" such as cursing or lewd remarks.

Forbid posting information related to criminal

(please turn to page 3)

IN THIS ISSUE

(continued from page 1)
behavior such as gambling. While that may seem far-fetched, it's not out of the realm of possibility to see an employee "brandishing a firearm or spray painting a house on YouTube."

Be prepared for the unexpected, he cautions. It can generate mischief nobody anticipates.

Even the attorneys can be at fault. On Facebook, it's not uncommon for a lawyer "to gripe about a client or about a partner or the administrator."

Or someone could breach confidentiality unintentionally by posting a comment about a case, and even if the client's name isn't mentioned, someone could recognize the issue and know who the client is.

Can the firm put restrictions of that type on its employees? Yes. If somebody gets on Facebook and slams a client or the partners, the firm "has a right to do something about that."

It can also prohibit conduct such as bad language and cursing because it harms the office's reputation.

And "any kind of conduct that's against the code of ethics of the bar association" can be prohibited.

As to employee rights, nobody can argue "I have a right to get on YouTube at work," he says. There's no case. Employment law requirements excepted, nobody has a right to anything at work.

PROTECT THE FIRM'S SYSTEM

Along with the policy, take technological precautions to prevent damage to the system and data.

Virus protection and firewalls are the first concern, because "a lot of criminals on the internet no longer use the traditional ways to cause havoc but are moving to Facebook."

Make it a rule that nobody can use a work-related password for a social site. The danger is twofold. One employee could access another's Facebook or Twitter account and damage the firm's image or reputation. Worse, an outsider could use the password to access the office's system.

Also make it a rule that everybody has to change passwords at certain times, because passwords can be discovered and it's via passwords that most criminal activity occurs.

And emphasize that the safest passwords are nonsensical letters, numbers, and symbols, not the obvious such as the name of a favorite sports team.

RESTRICT AND MONITOR

For the policy to have teeth, the firm has to restrict as well as monitor the social sites.

There needs to be a web filtering system to control what comes in. That allows the office to restrict each person's internet access on several levels. It can shut people out of certain sites. It can limit the access to certain times such as noon to 1:00 p.m. or after 5:00 p.m. And it can limit the access time each day.

There's also spyware to monitor everybody's activity, though the firm needs to tell employees beforehand that their communication may be recorded.

If there's protest, Weinblatt says, point out that the firm owns the computers and the information on them and has the right to access and control whatever goes through its own server.

Point out too that when an employee "uses the employer's tools" to create damage, the employer can be held liable.

AND LAY OUT THE CONSEQUENCES

Finally the policy needs to establish consequences. Include a statement that violations can result in disciplinary action, including termination.

And as with the sexual harassment policy, set out a complaint procedure and name a contact person for reporting internet bullying and harassing.

In addition, state that when a complaint occurs, the office will need proof, so anyone who makes a complaint should print out whatever is being sent so there's a paper trail of evidence.

Why the office needs job descriptions and how to get them all written

It's not fair to hire someone without explaining the requirements of the job – from the very large to the very small.

Neither is it fair to review a staffer without explaining what performance and behaviors the firm expects to see – from the very large to the very small.

Sadly, that happens all too often, says **BILL KAPLAN**, vice-president of operations for McNamara & Associates in Morganville, NJ. Many employers don't have job descriptions at all, and many more have descriptions "that haven't been updated in years."

With employment, "there should be no surprises," he says. Nobody should ever say "I didn't read a job description when I was hired." And no staffer should have to suffer through a review that covers points that weren't explained at the outset.

LET STAFF START THE JOB OFF

For any office that has zero descriptions or descriptions that are outdated, it's time to start afresh, Kaplan