Your Office Policies Need to Keep Pace with Technology

Maureen Waddle, MBA, and Derek Preece, MBA

As social networking and internet activities become ubiquitous in our society, practice management must make sure they keep abreast of the potential for technology to affect business.

About a year ago, there was a well-publicized story about the Philadelphia Eagles firing a six-year employee who worked the gate on game days. Why was he fired? He posted a comment on Facebook expressing concerns about the Eagles’ decision to let safety Brian Dawkins sign with the Broncos. Team management objected to being criticized by one of the employees and terminated his employment.

In the healthcare arena, the same challenges exist. One recent report told of a hospital in California that was seeking to terminate five workers for discussing patients in an online forum.1

As social networking and internet activities become ubiquitous in our society, practice management must make sure they keep abreast of the potential for technology to affect business. Practice administrators and physicians need to be aware of the many personnel issues arising from technology advancements, including these:

• Can I fire someone for negative remarks about the company on the employee’s social networking site?
• Do employees have a free-speech right to say anything in internet forums?
• Can I review social networking sites as part of the applicant review process?
• Can I access my staff members’ email messages?
• As an employer, what can I do to protect myself?

If you monitor the various advice forums, e-lists, and blogs for ophthalmic administrators you will find frequent posts of managers who have had employees post comments about work and/or patients on their social networks or blogs. You will also hear discussion of the use of online information in making hiring decisions. Because the use of technology changes so quickly, laws and court cases tend to lag behind, leaving practice administration wondering what is and isn’t appropriate in their relations with employees.

This purpose of this article is to raise your awareness about some of the issues touching on new technology as it relates to human resources within ophthalmology practices. However, be aware that this information is not comprehensive and that laws and interpretations are ever-changing in this area. What was acceptable last year may land you in serious labor law trouble this year, so it is incumbent upon every practice leader to keep up to date on both state and federal regulations and to have a trusted employment law attorney as an advisor for areas that are difficult to interpret.

Researching employment law through various legal journals and human resources journals yields these answers.

_Can I fire someone for negative remarks about the company on the employee’s social networking site?_

Any time you need to fire an employee, it is good practice to seek guidance from your attorney to make sure you do everything possible to avoid legal retaliation. If you are in an “employment at will” state, you are generally not required to have a reason to terminate an employment, provided it is not done for any prohibited reason (age, gender, religion, race, or disability; in some states sexual orientation is also protected). There have been cases, as mentioned in the case of the Philadelphia Eagles employee, where employees have been fired for comments made on social media sites. However, whether an employee could bring a successful legal action against you for termination in a similar case would depend on the specific facts of the situation and the legal environment in your state.

_Do employees have a free-speech right to say anything in internet forums?_

Many believe that the constitutional protections for free speech give them the right to say anything at any time. However, the first amendment only guarantees that “Congress shall make no law... abridging the freedom of speech, or of the press ...” The courts have usually allowed private industry to set policies and adhere to guidelines regarding employee behaviors, including moral conduct. Therefore, the employee has every right to his/her freedom of speech and every right to accept the consequences of such free expression including termination from employment. There are many blurred lines here, and again, “at-will” seems to protect most employers in their decision to terminate employees who harm the company in their internet endeavors. That being said, employers can run into trouble if they use coercion or deceit to obtain passwords or other login information in order to gain access to private blogs.

_Can I review social networking sites as part of the applicant review process?_

Social networking sites are considered voluntary and therefore open for viewing. According to a 2009 survey by the site CareerBuilder.com, 45% of respondents use social media sites to research applicants. Employers may not engage in illegal means to access the information or misrepresent their intentions to gain access to the information. While content that is considered provocative or that demonstrates illegal behavior may keep an employer from extending an offer, many employers have found that internet findings influence them in a positive fashion. Some indicate that after their internet research they extended offers because they were influenced by sites that showed the candidate to have a good personality fit or that the candidate demonstrated creativity, or the site corroborated previously stated qualifications.

For your own protection, it is probably best that you obtain written permission of potential candidates prior to researching their internet activities. Though such internet research permissions are not yet mandated, the Fair Credit Reporting Act requires an employee’s or applicant’s permission prior to a credit search, and it may not be long before online search permission is also required.

_Can I access my staff members’ email messages?_

In general, employers can monitor all email that is sent and received on the company email network. It is advisable to publish and enforce a policy stating that practice email is for business use only and that email messages will be monitored. Many practice personnel policies also state that practice equipment is only for company work and not for personal use, and some practices employ software to limit employees’ access to non-practice email.

continued on page 18
As employers, what do we do to protect ourselves?
First, be clear and transparent about your expectations regarding the use of technology at work by putting your policies in writing and having employees acknowledge receipt of that document. Ideas for policies regarding the use of technology can be found on various internet sites:
- www.instantsecuritypolicy.com/
  index.html
- www.biztree.com
- http://employment
  lawadvisors.com/
- www.unifiedcompliance.com
Be sure to have your employment attorney review and approve any policy language that you expect to be binding on your employees.

Second, once you have a policy, you must monitor and hold everyone to that same standard. If you knowingly allow some employees to disregard the rules or if you turn a blind eye to possible misuse, you may find that you set a precedent that prevents the application of that policy for other staff members.

Third, provide training and updates on appropriate behaviors and expectations of employees. To simply include a policy in a personnel manual is not enough to make sure your staff will appropriately apply that policy to their own actions. Since technology is evolving so quickly, employees need to be continually reminded of the parameters of your rules and how they apply to new online or mobile applications. It is particularly important to provide frequent reminders that discussing patient care online is inappropriate and may even be illegal, depending on what information is disclosed.

Finally, hire right. By hiring people with good reasoning skills and values that match your practice’s, you will avoid some of the problems that plague less vigilant offices.

Summing Up
Technology in the workplace has created new challenges for employers, but good legal guidance, clear policies, consistent enforcement, and ongoing training can help practices ensure that they comply with the laws and regulations that apply to this new world in which we live.

Note