# Social Networking In Schools

Insights
4.01.10

(Education Update, No. 2, April 2010)

As more students, parents, teachers and administrators tap into social networking sites such as Facebook, MySpace, Twitter and YouTube for educational, school communication, admissions marketing and other purposes, the lines between educational and personal networking are becoming more and more blurred.

Social-networking sites like Facebook and MySpace allow users to create personal websites and to post online personal information about their employer, marital status, friends, outside interests and hobbies as well as photographs and real-time "status" updates. Sites like Twitter allow users to send and receive short messages up to 140 characters in length. Better known as "tweets," these messages are displayed on the publisher's profile page. More and more people are using social-networking sites daily. For instance, Facebook's blog says that it has more than 400 million *active* users and that 50% of them log in on any given day.

There is no "one size fits all" approach to social media use in schools. Different schools use social-networking sites differently. Some schools do not use social-networking sites at all and may have filters that prevent employee and student use at school. Other schools use social media to communicate with parents and students by publishing a school newsletter or by providing "tweets" to parents about scheduling, weather closures and classroom updates. Some use social media for recruiting and evaluating prospective employees. Others use social media for alumni communication and fundraising. Some schools are using social media to enhance student learning because it enables students to connect and form virtual communities.

**The Risks Of School-Sanctioned Social Media Use**
As schools explore the positive ways that social media can be used in education, negative uses are sure to reveal themselves as well, presenting new concerns and legal risks for schools.

A teacher may "friend" a student, allowing that student to have unfettered access to the teacher's private life, the ability to post private information about students, or much worse, engage in inappropriate communication with a student. An employee may post negative comments or risqué photographs on a social networking site that also identifies the school.

A potential staff or faculty member's social networking site may reveal that person's race, religion, disability, or sexual orientation, thus exposing an employer to increased risk of a failure to hire claim. A positive LinkedIn recommendation that contradicts the reasons for a poor-performance evaluation may be used against the school in a later wrongful termination lawsuit. Employees have new avenues for harassment, disparaging other employees and the school, and sharing confidential information. Yet, taking adverse action against an employee based on information gleaned from a social-networking site may lead to invasion of privacy and other claims.

**Savvy Screening Method – Or Risky Recruitment Tool?**

More and more often, schools are turning to the Internet for information about potential new hires. Employers face a number of barriers when it comes to effectively screening job applicants. For example, many applicants fabricate their résumé and lie during interviews. While the Internet can certainly provide enlightening information about a candidate's attitudes, behaviors and core values, the risk of "social-media screening" may outweigh possible gain.

First of all, Facebook and MySpace profiles can indicate race, religion, disability, sexual orientation or other protected categories of an applicant, increasing the risk of a discriminatory failure to hire claim if the applicant is not hired. In addition, a savvy user of online media can manipulate information to create a false personal image.

Currently, there are no published discrimination cases based on an employer's use of social-networking sites to monitor employees or screen applicants. But given the increased use of social-networking sites in recent years, no doubt employers will soon find themselves in court being sued on allegations of discrimination or retaliation for taking adverse employment actions based on information obtained from social-networking sites.

Another concern for schools is the Fair Credit Reporting Act (FCRA) and its state equivalents. While FCRA generally does not apply to situations where a school uses social-networking sites on its own (i.e., without engaging a third-party background screening firm), it may apply to situations where an employer uses such sites in conjunction with certain workplace misconduct investigations.

Moreover, if a school does engage a third-party background screening firm and includes searches of social-networking sites as part of the requested background check, the employer would be bound by the provisions of the FCRA. Other state fair credit reporting laws may provide more protection to job applicants and employees, so be sure to review any state-specific statutes to ensure that your school is in compliance with all applicable laws.

**MySpace...My Privacy?**

Many employees feel that it is an invasion of privacy for employers to look at, and base employment decisions on, their social-networking profiles. This is likely due to the misperception that information posted on these services is private; many MySpace and Facebook users do not realize that the information they post can generally be viewed by the public. In most cases, employees will not be able to successfully argue that accessing their profile constitutes a cause of action for

not be able to successfully argue that accessing their profile constitutes a cause of action for invasion of privacy because an invasion of privacy cause of action requires a showing that the employee had a *reasonable* expectation of privacy in the content posted. An employee would likely have a difficult time establishing that reasonable expectation of privacy when thousands, if not millions, of people had access to the employee's profile and the employee voluntarily disclosed personal information in the public domain.

But it is not true that an employee stands no chance of successfully asserting a claim for invasion of privacy. The outcome might be different if, for example, an employee makes his Facebook profile "private," or for his "friends" only, and the employer is able to circumvent the privacy setting simply to obtain information for making personnel decisions.

Also, using information obtained from social networking sites may be problematic since some states, including California and Colorado, prohibit an employer from imposing discipline for lawful conduct – such as disparaging "tweets" and "wallposts" – conducted on a person's own time. Schools in such states may be exposed to potential liability if they choose to take adverse action against an employee after viewing photographs of the employee on the employee's profile, smoking, drinking, or engaging in other lawful conduct.

**Pop Quiz: Is Digital Information Protected By Privacy Law?**
Recently, a group of restaurant employees set up an invitation-only MySpace group called "Spectators" where they could "vent any BS ...without outside eyes spying on us." [*See "Off-Duty Discussion Groups Can Be Off Limits To Employers,"* in the March, 2010 issue of the Fisher Phillips Hospitality Update]. Postings referred to violence, illegal drug use and a posted copy of a required test for employees. A manager caught wind of the group and asked an employee for the password to gain access to the group – and then terminated employees for criticizing their bosses after viewing the online posts. When the case went to trial, the jury found the manager's actions violated federal and state statutes, which prohibited unauthorized access of electronic communications sites based on the way the password was obtained. *Pietrylo v. Hillstone Restaurant Group d/b/a Houston's*.

The lesson to be learned is that although employees should have no expectation of privacy when it comes to publicly available material, schools need to be extremely careful of how they obtain protected information they believe they have a right to know. Managers should not coerce employees or students to provide passwords or use "fake friend requests" as a way to try to access an employee's or student's private pages.

As the online barriers between the personal and school-specific use continue to blur, administrators and faculty must be increasingly careful when becoming "friends" with employees, students or parents in cyberspace. Online information and opinions can potentially lead to harassment, discrimination or other claims – even if posted on a personal profile. In one case, a manager posted two controversial comments on his personal Web page: "What's wrong with women these days?" and "Chicks seem to have more issues these days than Jet Magazine and keep up more drama than daytime TV and Jerry Springer combined." These postings were used by an employee to support her

lawsuit. *Derrick v. Met. Gov't of Nashville & Davidson Co.*

**To Ban Or Not To Ban?**

Since social-media use is so multi-faceted, no single approach will apply to all situations. Some schools may opt to place an outright ban on social-media access at school as well as prohibit "friending" parents, students and other employees. Other schools may simply prohibit employees from identifying their school online. As the use of social-networking sites for educational and community communication purposes increases, schools may need to adapt to the mainstream use of such sites and recognize that a blanket prohibition simply isn't practical. Regardless, your school should take action now to safeguard against social media mishaps.

All schools should have a social-networking policy. A computer-use policy that simply prohibits personal use and disclaims any expectation of privacy is not enough. While it is tempting to ban social networking altogether, this may raise enforcement problems particularly as schools take advantage of the opportunities of social media use in education.

Make sure that existing computer-use, confidential and proprietary information, and no-harassment policies (employee and student) specifically address social networking. Schools that check candidates' public social-networking sites should avoid "fake" friend requests and be consistent – if your school checks any candidate, check them all.

Advise your employees that if they use the school's email address or name they must act in accordance with the school's professional standards, including respecting the school, its employees, parents, students, etc. Continue to remind employees of the risks of unequal relationships when dealing with students. Provide training in order to ensure that employees understand that information posted on social networking sites may be public and also understand the school's policies.

Remind all employees, including administrators, faculty and staff of their heightened obligation not to reveal confidential information on-line and educate them about the risks of becoming on-line "friends" with parents, students and/or subordinates. Finally, consistently enforce such policies and before taking any disciplinary action, carefully investigate any suspected misconduct.

## *Service Focus*

FCRA and Background Screening