



Legal bytes – current hot topics in cyberlaw

Sara C. Clark, deputy director of legal services

One of the things I enjoy most about working in school law is that the job is never boring. The law is *constantly* changing and nowhere is that more apparent than in the area of technology.

The rapid speed of technological change means that laws and policies governing technology are out-of-date almost immediately after their passage, leaving even the most adept school districts struggling to handle issues that arise.

Let's take a look at a few of the "hottest" topics in this area, with suggestions for what school districts can do to stay ahead of the game.

Fired over Facebook

Just before the holidays, the National Labor Relations Board (NLRB) answered a question facing a growing number of employees: When can your Facebook posts get you fired?

The case — *Hispanics United of Buffalo* — started in 2010, when an employee named **Marianna Cole-Rivera** posted a comment on Facebook from her home computer. In the post, Cole-Rivera complained about one of her coworkers, who had accused her fellow employees of not helping their clients enough. Four other off-duty employees responded to the post from their personal computers, generally objecting to the assertion that their work performance was substandard. The following workday, the employer fired all five employees, alleging their off-the-clock comments had violated the employer's anti-harassment policy.

In addressing the case, NLRB applied

the National Labor Relations Act (NLRA), which generally establishes workers' rights to take collective action to improve their working conditions. This action is called "concerted activity" under NLRA. In analyzing whether activity is "concerted," NLRB typically examines whether other employees engaged in the activity, or whether it was solely by or on behalf of the employee. To be protected under NLRA, the content of the speech also must concern the terms and conditions of employment.

In this case, NLRB held that the terminations were unlawful because the employees' comments were the first step toward taking action against accusations about their performance that they believed the employee would make to management. NLRB found that the Facebook postings were concerted and protected, and because the employer discharged the employees based solely on their postings, NLRB found that the firings violated NLRA. NLRB wrote that by commenting on her Facebook post, "Cole-Rivera's four coworkers made common cause with her," and that "there should be no question that the activity engaged in by the five employees" fell under the labor law's protection.

The case confirms NLRB's position that social media comments will be analyzed in the same way that traditional oral statements have been evaluated. Moreover, NLRB's conclusion that the specific comments were "protected conduct" shows that the current NLRB is inclined to protect comments if they can possibly be construed as a first step toward group activity, regardless of

whether a union is involved.

The case serves as an important reminder to school districts to be cautious when considering discipline or discharge over employee comments made on social media. In addition, school districts should ensure that any social media policies in place are carefully drafted so they are not so broad as to prohibit employees from engaging in protected activity.

Storing data on 'the cloud'

The U.S. Department of Education's (DOE) Privacy Technical Assistance Center (PTAC) recently issued a frequently asked question (FAQ) document on the increasingly popular topic of using cloud storage for electronic data. Cloud computing typically involves using a network of remote servers hosted on the Internet to store data (rather than storing them on a local server or personal computer). Many districts are using cloud technology to store electronic data, such as student records.

PTAC was established by DOE as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality and security practices related to student-level longitudinal data systems. The FAQ document contains responses to questions about meeting necessary data privacy and data security requirements — including the Family Educational Rights and Privacy Act (FERPA) — and provides a short list of best-practice resources to ensure the proper protection of education records.

The FAQ document makes it clear that FERPA does not prohibit the use

of cloud computing solutions to host education records. FERPA permits a school district to disclose, without prior written consent, personally identifiable information from education records to a contractor, consultant, volunteer or other party if the school district meets certain conditions.

This exception to the requirement of consent in FERPA is often known as the “school official” exception and requires, among other things, that the school district maintain “direct control” over the use and maintenance of personally identifiable information from education records. To maintain this control, the FAQ document suggests that schools make clear in their service agreements or contracts that the outside party may not use or allow access to personally identifiable information from education records, except in accordance with the requirements established by the school district that initially disclosed the information.

The FAQ document also suggests that school districts use reasonable methods to ensure the security of their information technology (IT) solutions, including conducting a careful risk-management assessment before deciding whether this new technology is right for them. Some important considerations, according to PTAC, include:

- whether the cloud solution provides an appropriate level of security, such as firewalls, security monitoring and patch management procedures;
- whether the district needs to update its policies and procedures on record storage to accommodate the new system;
- how the district will exercise and manage control over the access and use of data;
- whether storing data on the cloud will interfere with the district’s ability to provide parents and eligible students with access to their records, as is required under FERPA.

A copy of the FAQ document is available online at <http://links.ohio>

schoolboards.org/54535. Schools considering a cloud solution should fully investigate these issues and work to ensure their education records remain protected and secure. A district’s IT employees will be helpful in this process. There also are outside technology


consultants and companies that can assist with this transition if the district needs additional support.

Board members’ use of social media

For the past decade, the public’s use of social media continues to rise, but

PayForIt.net




... *loved* by parents ...

| | | |
|---|---|---|
| <p>Registrations</p> <ul style="list-style-type: none"> • Fees • Activities • After School Programs <p>Fees</p> <ul style="list-style-type: none"> • Tuition • Book Fees • Class Fees • Etc. <p>Activities</p> <ul style="list-style-type: none"> • Swim Classes • Prom Tickets • Etc. |  | <p>Lunch Service</p> <ul style="list-style-type: none"> • Student Accounts • Auto Replenishment • Adult Menus <p>After School Programs</p> <ul style="list-style-type: none"> • Tutoring • Child Care • Etc. <p>Fundraisers</p> <ul style="list-style-type: none"> • Flowers • PTO Donations • Etc. |
|---|---|---|

... *needed* by schools ...

**Contact: Bob Reolfi, Esber Cash Register,
1-800-669-0792 or Bobr@ecrpos.org**

Endorsed By:

many school board members have been reluctant to use social media, fearful of and focused on the potential negative outcomes. There are some good reasons why board members should be skeptical of social media. However, when used correctly, social media can improve communication with constituents, increase opportunities for community engagement, enhance collaboration and the exchange of ideas and increase the public's access to information.

A board member's status as a public official may make some members reluctant to dive into social media. As public officials, board members are subject to a number of standards and requirements that do not apply to regular citizens. For example, the Ohio Open Meetings Act (Ohio Revised Code (RC) 121.22) requires public bodies in Ohio to take official action and conduct all deliberations upon official business only in open meetings where the public may attend and observe.

Although neither the courts nor the attorney general have weighed in on the issue of whether social media is

governed by the Open Meetings Act, an argument could be made that if a board member posts a comment on social media about board business and a majority of the other board members respond to the post, this may constitute a "meeting" under the Open Meetings Act. A conservative approach would be to have less than a majority of your members comment on any social media post.

Public records laws also may deter some public officials from using social media. As defined in RC 149.011(G), a public "record" includes any document, device or item, regardless of physical form or characteristic, including an electronic record, created or received by or coming under the jurisdiction of any public office of the state, which serves to document the organization, functions, policies, decisions, procedures, operations or other activities of the office. If the content of a board member's post or comment on social media meets this broad definition, it may constitute a record under Ohio's public records laws.

If it meets the definition of a record

and constitutes the board's official record (and not a secondary copy), the information must be retained in accordance with the board's records retention and disposition policy. To assist public entities with the challenges that accompany managing records created by social media, the Ohio Electronic Records Committee has published a document titled "Social Media: The Record Management Challenge." The document, which is available online at <http://links.ohio-schoolboards.org/75464>, serves as a resource for school districts to manage the creation, retention, disposition and preservation of social media records. School board members who use social media should review this document and ensure that they are properly managing their own social media content in compliance with Ohio's public records laws.

A final word of caution for board members interested in using social media: do not use social media to do something that you would not otherwise be able to do. For example, although it may be tempting to post photos of students at an assembly or the names of recent student award recipients, this information is likely protected student information under FERPA. Sharing employee health information or information discussed during executive session also are examples of inappropriate (and potentially illegal) posts on social media.

For more updates on technology and the law, please consider attending OSBA's annual Cyberlaw Workshop, which will take place at the OSBA office on March 15. To register, contact **Laurie Miller** at (614) 540-4000 or Lmiller@ohioschoolboards.org, or visit www.ohioschoolboards.org/cyberlaw-workshop. ■

"According to law" is designed to provide authoritative general information, sometimes with commentary. It should not be relied upon as legal advice. If legal advice is required, the services of an attorney should be obtained.

Are you currently involved in litigation that may have statewide significance?



The OSBA Legal Assistance Fund (LAF) is available to provide financial or legal assistance in matters of statewide importance to local school districts.

LAF offers direct financial assistance or other support in the form of amicus curiae briefs.

Please call OSBA at (614) 540-4000 or (800) 589-OSBA for information about your member status or to obtain an application if you have a pending matter that may meet the above description. Visit www.ohioschoolboards.org/legal-assistance-fund for more information.