



Free Speech in a MySpace World

By Steven M. Baule and Darcy L. Kriha

In the potential shadow of a “Bong Hits for Jesus” banner, complicated student speech and discipline issues arise almost daily on the Internet. Whether it is a mock MySpace page set up to make fun of a teacher or a direct threat to an assistant principal, it is often unclear exactly where school ground discipline ends and student free speech rights begin. Ever since *Tinker v. Des Moines Independent Community School District* (393 U.S. 503) was decided by the U.S. Supreme Court in 1969—with its seminal holding that students do not leave their constitutional rights at the “school house gate”—administrators, teachers, parents, and students have continued to explore the scope of student free speech rights on school grounds and at school events. The Internet and advances in technology have dramatically changed the variables of student speech issues.

question has a disruptive impact on the educational environment. If a student adds a slanderous set of comments to RateMyTeacher.com and the teacher in question reads the comments and is truly bothered by it, is there a disruption of the educational environment? Does it matter if the teacher accesses the site from home or from her classroom? How does the impact of the comments change if the student e-mails or instant messages all of her friends and tells them to review the site? Does it matter if the student sends those messages at home or during study hall?

When Concerns Arise

What should you do when a student Internet speech issue arises? The first action is to document the Web site, MySpace page, or e-mail. The extremely fluid and transitory nature of electronic

your building administrator and your technology director to determine the next steps to take with student discipline. Two basic issues need to be addressed. The first issue is whether or not the speech can be directly linked to one or more students. The second issue is whether or not the speech in question warrants school discipline. Courts have held that school discipline (e.g., in-school suspension, out-of-school suspension, and even expulsion) is defensible in instances where the student’s speech has a tangible negative “nexus” or connection to a school and/or the educational program.

Your building administrator, potentially in consultation with a school attorney, will need to decide whether the speech in question creates the nexus that can lead to disciplinary action. In order for the speech to be disciplined, it must be a specific threat to a student or staff member or the school as a whole and/or disruptive to the educational environment. Schools have an obligation to treat threats seriously. Whether or not the threat is made from a school computer or a home computer, anything perceived as a legitimate threat should be acted upon by school and potentially law enforcement authorities. The question becomes, what is a legitimate threat?

“The Internet and advances in technology have dramatically changed the variables of student speech issues.”

Identifying the Issues

Many, if not most, adolescents utilize electronic social networking sites as a primary method of communication and as a way of expressing themselves and displaying their thoughts, feelings, and ideas. Most of the time, social networking sites provide adolescents and young adults viable and healthy methods of self-expression. However, when those sites are used to propagate disruptive, slanderous, or even threatening speech, educational environments are often impacted.

The primary concern of such electronic speech is whether or not the speech in

communication makes immediate documentation of the offending speech essential. If you receive an e-mail or find a Web site containing student speech that is questionable, print a hard copy and save an electronic copy, if at all possible. Screenshots of the offending document that are date/time-stamped are particularly useful. Capturing the offending text is particularly important for Web sites, since they can be changed instantaneously; simply bookmarking the offending site will not ensure that the content will remain in place.

Once you have created a hard copy and potentially one or more electronic copies of the offending speech, contact

What the Courts Have Said

If a student’s MySpace page is soliciting funds to hire a hitman for Mrs. Smith or Mr. Price, is that a threat? It may be perceived as one by Mrs. Smith, particularly if she recently failed the student. However, what if the MySpace page was marked private and only the student’s 23 “friends” were allowed to view it, but it was accidentally left open on a computer in a classroom? What if it was Mrs. Smith’s classroom? Each of the above questions will have to be weighed in determining whether or not the student should be disciplined.

“Administrators, IT staff, library media staff, and teachers must be aware of what constitutes genuinely inappropriate behavior for which disciplinary action is appropriate and what are simple cases of adolescents expressing their free speech.”

Unfortunately, there are few black and white answers in the world of 0s and 1s. In *J. S. v. Bethlehem Area SD* (807 A.2d 847, Penn. 2002), the court upheld the right of the school to discipline a student for a similar action. The teacher in the case was so distraught that she had to take a medical leave. The fact that the teacher was affected in this manner undoubtedly influenced the court.

In another case, *Killion v. Franklin School District* (136 F. Supp. 2d 446, Penn. 2001), a student was suspended for sending an e-mail top ten list articulating in a derogatory and lewd manner all that was wrong with the athletic director's appearance. However, it was not done at school or on school time and the list wasn't generally circulated at school. In that case, the court overruled the student's suspension because the speech did not materially disrupt the school.

In a third case, a student created a MySpace parody about the principal that included some profanity. It received so much student attention at school that the technology director had to shut down the school's computer network to install a new firewall. Classes were canceled and students were unable to complete their work using the school's computers. The court found in *Layshock v. Hermitage SD* (412 F. Supp. 2d 502, Penn. 2006) that the school was correct in disciplining the student due to the disruption caused to the educational process as a whole.

Other considerations may include: was the offending speech found by searching the Internet or did it come to light on its own? Did the speech appear on the computer screen or printer without being sought by the staff? How many students or staff members were aware of the speech? A staff member who goes out and checks MySpace and FaceBook for speech she finds offensive is generally not in the same position as a teacher whose students tell her about the offending speech during her study hall assignment. Is the speech clearly

identified as a parody, or is it an attempt to impersonate the intended victim? If a student lists a teacher on Craigslist under the Erotic Services section and lists her actual home and school phone numbers along with her yearbook picture, is that the same as if the student uses her picture in sending a fake prostitution ad out to his friends via e-mail? What if the teacher's voicemail is filled with people looking to meet a prostitute?

There are many grey areas within the realm of student speech in the electronic age and especially in social networking sites. Stay informed and speak with your administration, professional organizations, and school attorneys regularly to stay up to date.

Practical Issues and Actions

Your technology staff will need to gather the information to track and identify the user or users who created or disseminated the speech in question. In cases of hate speech or other possible threats that could potentially result in criminal prosecution, you may want to contact your local police department. Many police departments have either Internet crime units or officers identified and trained to work on Internet and computer networking cases. It is often possible to track Internet transactions to a specific IP (Internet protocol or TCP/IP) address or even to a specific MAC (machine) address, if the tracking is begun immediately. Usually this can

Introducing the First MP3 Player Designed for Schools!

Now the personal media players your students love can be part of their learning environment—thanks to the new Califone® MP3 Player:

Maximum playback volume level (85db) and ambient noise reducing earcups on the headphone for **hearing safety**—meet American Speech-Language-Hearing Association (ASHA) guidelines.

Industry-first **dual headphone jacks** for multiple listeners—supports individual & group learning and stretches your technology budget!

Microphone for podcasting, recording vocal responses, testing & tracking student progress.

Durable, **easy-to-use**, and made of rugged ABS plastic to meet the demands of classrooms & libraries.

Ideal for **nurturing language learning & reading skills**, ELL, ELD applications and listening to recorded books and music.

FREE Shipping for MP3 Players Purchased Through Authorized Califone® Dealers Until June 2008!



CALIFONE
The Sound of Education™
califone.com

“Courts have found that one-time notification about acceptable use may not be often enough, making it a good practice to ask students to sign an AUP each year.”

be done within a limited timeframe, depending upon how various logs are kept on different systems. Seven days tends to be the time after which recovering information becomes difficult.

In addition to the server, router, and firewall logs, a large amount of information is retained on the individual computer concerning which Web sites users accessed and when. At the simplest level, checking the history file of Internet Explorer will reveal where the user has been. Contrary to the assertions of some who have been caught going to inappropriate Web sites, pornography rarely “just pops up” on school computers. These logs can help identify when specific sites were accessed. In schools where students are required to log into a computer or sign into the library media center or other area, the two sets of logs can be used to identify the individual responsible or at least to significantly narrow the number of students in question.

Firewall logs usually list all the traffic by type (http, ftp, etc. or port number, 80 for http) and IP address. This may assist you in determining who was updating their MySpace page from the school or who was downloading that manual on creating a new virus. Similarly, if you know the hard-coded MAC address of the network card in the laptop that was stolen from the school, theoretically you could track that address to a given IP address and visit that Internet Service Provider (ISP) and work with them to define the exact location of your stolen laptop. Such a process culminated in the arrest and prosecution of a former teacher who had stolen six laptops from a school a couple of years ago.

Some schools routinely add key capture software to record each keystroke made on a specific computer. In cases where computer vandalism or other inappropriate use is common, such key capture software may be a wise investment. Such software would allow nearly 100% accurate identification of the user account being used to violate the school’s Acceptable Use Policy (AUP). Of course, the individual may claim they gave someone else

their password, etc., so it is not 100% reliable to identify the users themselves. Remember that key capture software is not foolproof and can be hacked into. Such hacking has been used by students to obtain credit card information, etc., from teachers or other students who are shopping online or doing personal banking during planning periods.

In many cases, it will be possible to determine the computer(s) involved in a particular incident and often the individual user account(s) used. This is especially true if the incident is caught immediately. However, if you do not have good user account and password security, it will be more difficult to identify the actual individuals involved.

Password security in its most simple form means ensuring the passwords used are not words that can be found in the dictionary nor should they be easily identifiable dates, e.g. birthdays, anniversaries, etc. The names of your children and pets are also good examples of poor password choices. Most computer security experts would suggest a password at least six characters long and including one or more special characters (!, @, #, \$, etc.).

Another key concern is to ensure that your school maintains its computer accounts in a timely manner. In many cases, students obtain the ID and password of a student teacher or even a retired teacher who is no longer employed, but their accounts have not been disabled. Often, such accounts are exploited for inappropriate use. Work with your IT and human resources staff to ensure there is a systemic method for removing old accounts and disabling access for those who should not have it. A simple method is to put an expiration date on each and every account created. For students and student teachers, it could be tied to the end of the semester or school year. For staff members, it could be tied to their probationary period. These dates can be batch modified in most systems, so it is not unduly burdensome to the IT staff and creates a much more secure computer network for your school.

Updating Your AUP

It is also important to ensure that your school or district has a comprehensive Acceptable Technology Use Policy (AUP) in place at the beginning of every school year, so that if students do misuse school technology or use the Internet as a conduit for inappropriate or illegal activities, the school will be able to take disciplinary action. Having students (and parents) agree to an AUP should be an annual practice in each school. Courts have found that one-time notification about acceptable use may not be often enough, making it a good practice to ask students to sign an AUP each year. Similarly, the IT staff may want to provide a summary of the AUP as a log in screen to computers a couple times a year, so that students and staff see the basic concepts behind the AUP at least each semester. This can be done via a login script in most network operating systems.

In making decisions about student speech via the Internet, it is important to ensure that the necessary technology is in place to audit and secure the school’s computer systems. Similarly, administrators, IT staff, and library media staff, along with teachers, must be aware of what constitutes genuinely inappropriate behavior for which disciplinary action is appropriate and what are simple cases of adolescents expressing their free speech. ■

Steven M. Baule is the superintendent of schools for the Westmont Community Unit School District 201 in Westmont, Illinois. His latest title from Linworth is *Facilities Planning for School Library Media and Technology Centers, 2nd Edition* (2007).

Darcy L. Kriha is a partner at Franczek Sullivan P.C. in Chicago, Illinois. She represents public school districts and special education cooperatives throughout Illinois. In addition to overall school board representation, Ms. Kriha is known for her expertise related to special education and high-profile student discipline matters.