Comprehensive social media policies and practices enable public school administrators to harness the benefits of social media while mitigating their risks.

Many teachers view Facebook, MySpace, Instagram and other social media as exciting teaching and learning tools that can help students build on skills and concepts introduced in school, bridge the gap between in-school and out-of-school learning, and improve competencies in technological skills needed for the 21st century. Teachers also say social media promotes collaborative learning, cross-cultural communications, language skills and creativity.

Despite social media’s relevance among the student population, public school administrators struggle with including these technologies in their classrooms, in part, because of the risks they pose. Social media can be misused by teachers who overstep the boundaries of their positions or by students who engage in cyberbullying, sexting or other inappropriate behavior. This misuse has led to outright bans of social media by some school administrators, while others have taken a less restrictive approach.

Being aware of the exposures and incorporating clear policies and guidelines for social media use, including a plan for thoroughly addressing misuse, can help schools manage the exposures social media tools present.

Social media exposures

Cyberbullying
The American Academy of Pediatrics describes cyberbullying as using digital media to deliberately communicate false, embarrassing, or hostile information about another person. A school can be held liable if it is informed about the harassment and fails to adequately address the situation. Bullying claims against schools have generally centered around students’ rights to a free and appropriate education.

Cyberbullying is a challenging exposure for schools because students’ many points of media access make it difficult to monitor and control. Cyberbullying can take place using school-owned resources such as lab computers or laptops, through wired or wireless school networks, or on personal devices used on school grounds.

Sexting
Likewise, a school has a responsibility to prevent or defuse a hostile environment that might develop as a result of sexting—sending nude or semi-nude photos via digital media—even if a student initiates the communication. Such messages, especially those that become widely circulated, can be classified as sexual harassment.
Investigating an act of sexting forces administrators to walk a precarious line, with potential legal ramifications involving improper search and seizure, distribution of sexually explicit images, and child abuse and neglect. Searches of student property must be reasonable, based on a strong suspicion that a search will uncover evidence of a violation of the law or school policy. In addition, if a sexting image is considered pornographic, possession or distribution of it could expose administrators to charges of child pornography and, under some state laws, may constitute child neglect or abuse.

Inappropriate behavior
Social media gives educators direct and often unmonitored access to students. Casual and impromptu, these online communications can blur the lines of appropriate student-teacher relationships. The resulting liability exposure from such interactions is often ambiguous. An employer is not automatically responsible for unlawful acts of its employees under the legal theory vicarious liability since the acts presumably occur outside the scope of employment. However, administrators may be legally responsible if found to have permitted the activity to continue.

Cyberbaiting
Cell phones in the classroom have enabled another emerging trend known as cyberbaiting. In this form of harassment, students taunt a teacher to the point of an outburst, then capture the tirade via a cell phone video, which is often posted online. The exchange may open administrators up to employment liability exposures if they wrongfully discipline, suspend or dismiss a teacher, particularly if that teacher was harassed on a regular basis. Limiting cell phone use in the classroom and talking to students about the issue, as well as having specific procedures for investigating cyberbaiting incidents are key to avoiding them.

Comprehensive policies matter
A comprehensive social media policy developed by a representative team of stakeholders, reviewed periodically and shared with the community, is key to mitigating social media risks. The National School Board Association (NSBA) advises that social media policies should pertain to all types of technology, both personal and district-owned, and should spell out acceptable behavior regarding all types of conduct, from cheating to disruptive classroom behavior.

The NSBA also recommends seeking parental permission before communicating with students via social media and encouraging teachers to separate personal and professional social network profiles. Policies, NSBA advises, should include provisions for educating staff, students and parents about privacy practices and appropriate use of social media tools.

Tools help manage risk
Along with adopting strong policies and guidelines, administrators can take steps to limit social media access by equipping staff and students with electronic devices that filter Internet access or by subscribing to educational social network sites with built-in security like Edmodo, Gaggle or echalk®. On most sites, teachers can supervise communication and interaction among students and also limit students’ communication to within the class, school or district. Other sites have mechanisms that block inappropriate language, detect threatening language and identify pornographic material.

Exposure Checklist

- Is there a social media policy in place for staff and students that specifically addresses behavioral expectations, management procedures, and consequences of non-compliance?
- Are all of the social media technologies used in the school district outlined in the social media policy?
- Is the policy reviewed and updated periodically to keep pace with ongoing and expected advances in technology?
- Does the policy clearly state that personal devices may be confiscated and not returned should they contain evidence in the event a crime is committed?
- Are teachers, staff and students routinely trained in the proper usage of social media sites? Is this training documented?
- Is there effective monitoring in place to detect instances of technology misuse on school networks?
- Does the school have a clear, established reporting process relating to problematic interactions with students?
- Are procedures in place for investigating and managing instances of social media misuse?
- Are responsible technology use messages incorporated in all field trip and overnight trip permission slips?