Acceptable (and Unacceptable) Uses of Technology

BY SARA GOLDSMITH SCHWARTZ AND SUSAN E. SCHORR, SCHWARTZ HANNUM PC

ith the fall semester in full swing, at least one new app or popular website is probably preoccupying students' time on campus. Remember YikYak from earlier this year? How about Prepfessions from 2013? Inevitably, some new technological tool will surface during the 2014-2015 school year to cause independent school faculty and staff to scratch their heads, or worse, fear that cyber-bullying may be more easily perpetrated.

As in so many other situations, a school's best offense is a strong defense. A well-drafted acceptable use policy (AUP) signals to students and parents that a school will not tolerate inappropriate or malicious use of technology. In order to be effective in both deterring unacceptable cyberbehavior and providing schools with a basis for discipline, the AUP should work in tandem with an AUA (acceptable use agreement), signed annually by students (and often parents, too), and should include the following elements.

Broad Principles. Precisely because technology and software evolve so quickly, the AUP should include foundational principles that apply regardless of the particular technology being used. An AUP should apply to cyber-activity that takes place via equipment or a network, whether owned by the school or student, and whether conducted on or off campus, during the school day or at night, and even on vacation, for as long as a student is enrolled. Thus, if a rising 10th-grader engages in sexting over the summer, the "sexter" may be held accountable by the school.



Announcement of Monitoring.

While accessing the school's network, using the school's equipment or their own, students should have no expectation of privacy. Schools cannot, and should not, monitor equipment and networks not owned by the school (unless the equipment is using the school's network); however, schools should engage with parents and encourage them to monitor students at home. Parents should be encouraged to bring concerns to the school. The AUP should inform students that the physical definitions of "home" and "school" have no relevance to cyber activity, if the cyber conduct is detrimental to the school experience of one or more students.

Teacher/Student Boundaries. Social media is now part of many classroom experiences as well as faculty-sponsored extra-curricular activities. Coaches may find it easier to text students about changes in practice times rather than email the team via a listsery that students seldom check. The risk is that these more informal practices create opportunities for adults and minors to interact casually, one-on-one. Schools should consider how best to adapt the AUP to the school's culture and activities, while minimizing the risks of inappropriate conduct between students and faculty.

In addition, each school should tailor its AUP to the ages of its students, addressing issues such as whether educational games are permitted, whether cell phones can be used during the school day or in particular areas of campus, etc. Ultimately, an ideal AUP will assist the school in ensuring that faculty and students are responsible cyber citizens, wielding technology for good and not for evil. ■



Sara Goldsmith **Schwartz** is founder and president of Schwartz Hannum PC, a law firm based in Andover, Massachusetts. With

the largest education practice in New England, the firm provides comprehensive guidance to the full spectrum of independent school, college and university clients. Sara is a frequent speaker at seminars for attorneys, human resources professionals and school administrators.



Susan E. Schorr is an attorney at Schwartz Hannum PC and counsels independent schools on a variety of student, parent and governance

matters. She contributes to the firm's Education Blog and speaks frequently at national conferences.