Students are frequent users of the Internet and other technologies — sending e-mail, creating websites, posting personal news in blogs, sending text messages and images via cell or smart phones, contacting each other through instant messages, posting on social networking sites (e.g., MySpace, Facebook, Xanga), posting videos on YouTube and posting to discussion boards. While these technologies provide valuable educational and communication tools for students, they also have given tech-savvy students a new venue to harass or intimidate peers or school staff.

The challenge for schools is not only in identifying and stopping such conduct so that students and staff feel safe at school, but determining the limits of their authority when the so-called “cyberbullying” is initiated outside of school and during non-school hours.

What is cyberbullying?

“Cyberbullying,” sometimes referred to as Internet bullying or electronic bullying, is defined in Education Code 32261 and 48900(r) for purposes of student discipline as an act of bullying committed through the transmission of a message, text, sound, or image by means of an electronic device, including, but not limited to, a telephone, wireless telephone or other wireless communication device, computer or pager.

Examples include:

- sending mean, vulgar or threatening messages or images;
- posting sensitive, private information about another person;
- pretending to be someone else in order to make that person look bad; and
- intentionally excluding someone from an online group.

Like other forms of bullying, cyberbullying is an effort to demonstrate power and control over someone perceived as weaker. It sometimes involves relationships, sometimes is based on hate or bias (e.g., based on race, religion, sexual orientation or physical appearance) and sometimes is perceived as a game by those who are the perpetrators.

Cyberbullying may be a carryover of verbal or physical bullying that is occurring during or outside of school. Other times, students who are victimized at school retaliate online and become cyberbullies themselves.

Why do people do things online that they would never do in real life? Researchers have theorized that when people use the Internet, they perceive they are invisible and anonymous. This is not true because most online activities can be traced. However, if someone perceives he or she is invisible, this removes concerns about detection, disapproval or punishment. Also, the lack of face-to-face contact leads to less empathy by the perpetrator toward the victim and results in the misperception that no real harm has resulted.¹

Extent of the problem

Research findings on the prevalence of cyberbullying vary depending on the age and gender of the children included in the study and the specific behaviors defined as cyberbullying or online harassment. Some recent studies have found:

- Nearly a third (32%) of online teens ages 12-17 have experienced some form of online harassment, such as having had private material forwarded without permission (15%), receiving threatening messages
(13%), and/or having a rumor spread about them online (13%).2

- 26% of teens have been harassed via cell phone, either by voice or text.3

- The greatest prevalence of cyberbullying occurs during the mid-teens (ages 14-17).4

- Adolescent girls are more likely than boys to have experienced cyberbullying in their lifetimes (25.8% vs. 16%) and to have cyberbullied others during their lifetimes (21.1% vs. 18.3%). The type of cyberbullying tends to differ by gender, with girls being more likely to spread rumors while boys are more likely to post hurtful pictures or videos.5

- Children of all races and ethnicities are vulnerable to cyberbullying victimization and offending. White students are somewhat more likely to report having been cyberbullied sometime during their lifetimes, but students’ reports that they have been cyberbullied within the previous 30 days are evenly distributed across race.6

- Students who are bullied in cyberspace are also more likely to be bullied at school, and to be perpetrators of cyberbullying themselves.7

How does cyberbullying impact victims and bullies?

Although many students report that they ignore or are not bothered by the cyberbullying (as much as one-third to one-half of victims depending on the study), for other students the effects of cyberbullying can be traumatic. Like other traditional forms of bullying, cyberbullying has been shown to cause psychological and emotional harm to youth and to affect school attendance and academic performance. Low self-esteem, depression, anger and, in extreme cases, school violence or suicide have been linked to bullying.

A recent study of middle school students who had experienced cyberbullying found that both boys and girls are likely to report feeling angry, sad and embarrassed, while significantly more boys are scared as a result of cyberbullying. The same study found a connection between victimization and lower self-esteem and higher suicidal ideation.9

Schools need to be equally concerned about the health, welfare and education of the students who are the perpetrators of cyberbullying. These students have been shown to suffer from many of the same psychological and emotional difficulties as their victims — such as low self-esteem, anger and social isolation — and to exhibit other problem behaviors such as drinking alcohol, using tobacco, getting into frequent fights and performing poorly academically.10

Even when students are engaging in cyberbullying outside of school, the participants may be together in school and so the activity may impact the school climate or interfere with the ability of students to be successful in school.11

Both perpetrators and victims of cyberbullying view their school climate more negatively than other students, with perpetrators of cyberbullying giving their school’s climate the lowest rankings. According to the researchers, “The question remains: do cyberbullying behaviors create a poor school climate or does a poor school climate foster a culture where cyberbullying behaviors are acceptable?”12

Legal issues regarding off-campus conduct

Board policy and administrative regulations pertaining to cyberbullying and resulting discipline should distinguish between bullying initiated on school campus using school equipment and systems and bullying initiated by students off campus during non-school hours. Districts and county offices of education have the authority to monitor their own systems and to take away computer privileges and impose discipline for improper use. However, questions continue to arise regarding how far districts/COEs can go in disciplining students for their off-campus conduct. The need to protect students and staff from harm must be balanced with students’ First Amendment right to freedom of speech.

Education Code 48950 provides a free speech right based on what a high school student may do outside of the school environment. That is, if the student’s off-campus speech or communication is protected free speech, no discipline may be imposed unless, pursuant to Education Code 48907, the expression is “obscene, libelous or slanderous” or “material which so incites students as to create a clear and present danger of the commission of unlawful acts on school premises or the violation of lawful school regulations or the substantial disruption of the orderly operation of the school.”
A number of disputes regarding this question have landed in the courts. In an unpublished case in 2009 (J.C. v. Beverly Hills Unified School District), a California federal court held that a district may discipline a student for off-campus conduct only if the conduct (1) impacts school activities or is brought to the attention of school authorities, and (2) causes, or is foreseeably likely to cause, a substantial disruption of school activities. In this case, the student recorded a video insulting another student. The video was created off campus, not using district equipment, and was posted on YouTube. The court found that the discipline imposed on this student was not justified because the district did not present evidence of specific facts that led school officials to predict that the video would cause substantial disruption at school. The video was not threatening and did not lead to any confrontation between the students. The court stated that “substantial disruption” goes beyond ordinary personality conflicts, hurt feelings or embarrassment that occurs among middle school students.

Other court decisions from across the country, although not directly applicable in California, underscore the difficulty in disciplining a student for off-campus conduct. For example, in Layshock v. Hermitage School District (2010), a Third Circuit Court of Appeals ruled that a Pennsylvania school district violated the free speech rights of a high school student who was disciplined for creating an off-campus parody MySpace profile of the school principal. The student had downloaded the principal's photograph from the school’s web site and created what the district considered to be a vulgar, lewd and offensive profile, which other students began accessing on school computers after hearing about it. Nevertheless, the court found that the relationship between the conduct and the school was so attenuated that it could not allow school authorities to “reach into a child's home and control his/her actions there.”

On the other hand, in J.S. v. Blue Mountain School District (2010), the Third Circuit Court of Appeals ruled in favor of a school district that had disciplined a student for creating an off-campus fake MySpace profile of a principal which used profanity and depicted the principal as a pedophile and sex addict. Even though substantial disruption in school activities had not yet occurred, the court was sufficiently persuaded that the profile presented a reasonable possibility of a future disruption.

Recognizing that the court reached opposite conclusions in two cases with seemingly identical legal issues, the Third Circuit vacated the two decisions and held a new hearing on June 3, 2010. Once the new ruling is issued, either side could request that the U.S. Supreme Court grant review.

These court decisions, and others that are beginning to emerge, illustrate the need for districts/COEs to proceed cautiously when considering student discipline for off-campus conduct, consult with legal counsel, and document, with specific examples, how the speech significantly disrupted, or was likely to disrupt, school activities or the targeted student’s educational performance.

Policy considerations

Board policy on cyberbullying should be considered in the context of an overall approach to school safety and discipline, with the goal of providing a positive school environment that maximizes student learning. Strategies to address bullying, including cyberbullying, may be incorporated into the comprehensive safety plan.

In developing policy on this issue, the governance team may wish to seek input from school safety committees, school site councils, students, parents/guardians, administrators, teachers, education technology staff and other technology experts, classified staff, and/or community organizations. Legal counsel also should be consulted, particularly regarding issues of student discipline.

CSBA’s sample policy BP 5131 - Conduct provides optional language which prohibits cyberbullying and addresses the school’s response in the event that cyberbullying occurs. AR 5144.1 - Suspension and Expulsion/Due Process reflects Education Code 48900(r) which authorizes the suspension or expulsion of a student who engages in harassment or bullying by electronic means. BP/AR 6163.4 - Student Use of Technology prohibits use of the school’s technological resources to engage in cyberbullying. Governance teams are encouraged to review these materials and adapt them to meet their unique circumstances. They might also wish to review the following related policies and administrative regulations: BP/AR 0450 - Comprehensive Safety Plan, BP 5137 - Positive School Climate, BP/AR 5145.12 - Search and Seizure (with respect to searches of students’ personal property and district property under their control), BP 5145.3 - Nondiscrimination/Harassment, BP/AR 5145.7 - Sexual Harassment, BP 5145.9 - Hate-Motivated Behavior and BP 5145.2 - Freedom of Speech/Expression.

As governance teams develop, review or revise policies or administrative regulations related to cyberbullying, they might consider the following issues:

- **Education of students, parents and staff.** Because cyberbullying often occurs away from adult supervision, students must be informed about the dangers of cyberbullying, what to do if they or someone they know is being bullied, the board’s policy pertaining to appropriate use of the school’s technological resources and the consequences of improper conduct. Instruction
might also be provided in the classroom or other school settings to promote communication, resiliency, social skills, assertiveness skills and character education.

Similarly, school staff and parents should be informed about how to recognize warning signs of harassing/intimidating behaviors and provided with effective prevention and intervention strategies.

- **Acceptable use of the school’s technological resources.** Districts/COEs have a duty to exercise reasonable precautions against cyberbullying that occurs while using school equipment. Board policy, as well as the Acceptable Use Agreement which students and their parents are usually required to sign as a condition of using the school’s technological resources, should include an explicit statement that prohibits the use of the school’s resources to bully or harass other students or staff.

- **Use of filters to block Internet sites.** The district/COE may have already installed on its computers a technology protection measure that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors. However, these measures should not be over-relied upon as a tool in preventing cyberbullying. Many districts/COEs have blocked access to social networking sites.

- **Supervision and monitoring of students’ online activity.** Reasonable precautions against cyberbullying should include supervision of students while they are using the online services of the district/COE. Classroom teachers, computer lab teachers, library/media teachers, teachers’ aides, other staff or volunteers overseeing student use of online services should understand their responsibility to closely supervise students’ online activities and should receive training or information about the board’s policy on acceptable use.

In addition, districts/COEs have the right to monitor the use of their equipment and systems. If they receive federal Title II technology funds or E-rate discounts, they are obligated under 20 USC 6777 or 47 USC 254 to enforce the operation of technology protection measures, including monitoring the online activities of minors. Governance teams should discuss how such monitoring will be accomplished, including whether they wish to track Internet use through personally identifiable web monitoring software or other means.

Maintenance and monitoring of the online services should be routine, technical and conducted by appropriate staff. Some districts/COEs use “intelligent content analysis” which monitors all Internet traffic and reports on traffic that has elements that raise a “reasonable suspicion.” Staff can then review those reports. Another technical approach allows for real-time remote viewing of any computer monitor in the building.

Students should understand that there is no expectation of privacy and that use of school resources can be monitored. Clear notice of this fact may deter improper activity.

The law regarding searches of an individual student’s Internet use and computer files, even when there is reasonable suspicion that a student has violated board policy, is complex. Staff is advised to consult legal counsel before conducting any such searches.

- **Mechanisms for reporting cyberbullying.** Students should be urged to notify school staff, their parents or another adult when they are being cyberbullied, they suspect that another student is being victimized, or they see a threat posted online. However, because students are often reluctant to report such incidents to an adult, in part because they fear retaliation by the perpetrator or his or her friends, the governance team should consider ways that students can confidentially and anonymously report incidents.

- **Assessment of imminent threat.** District/COE procedures for responding to a report of cyberbullying should include processes to quickly determine the legitimacy and imminence of any threat. Often, what initially appears to be an online threat may actually be meant as a joke or may be an online fight (“flame war”) that is unlikely to result in any real violence. However, the highest priority is to protect against a possible real threat, including notifying law enforcement as appropriate.

- **Investigation of reported incidents.** Site-level grievance procedures already in place for other types of harassment may provide an effective method for reporting and handling complaints of cyberbullying. The student who is being victimized should be encouraged to not respond to the cyberbullying and to save and print out the messages (with full e-mail headers) or pictures as evidence rather than deleting them.

The investigation should include efforts to identify the individual who is harassing the student. There may be a way to track him or her through the Internet service provider, even if the individual is using a fake name or someone else’s identity. If the district/COE suspects that the cyberbullying is criminal, local law enforcement may be asked to track the individual’s identity.
If it appears that the cyberbullying is initiated off campus, it will be necessary to show that the behavior has caused or is likely to cause a substantial disruption in order impose discipline on the student perpetrator (see section “Legal Issues Regarding Off-Campus Conduct” above). Thus, the investigation should also include processes for assessing and documenting the impact of the cyberbullying on students, staff or school operations.

• **Appropriate response to incidents of cyberbullying.** Depending on the seriousness of the harassment, responses might include notifying the parents of both the victim and perpetrator, filing a complaint with the Internet service provider or social networking site to have the content removed and/or the student’s user privileges revoked, using conflict resolution procedures, suspending or expelling the perpetrator, and/or contacting law enforcement if the behavior involves a possible crime. The student perpetrator and his or her parents should be informed of the potential consequences to which they may be subjected, including potential civil law liabilities.

In addition, the district/COE should consider ways it can provide support to the victim through counseling or referral to mental health services.

---

**Resources**

**California School Boards Association:** CSBA issues sample board policies and administrative regulations, advisories, policy briefs and publications on a variety of topics related to school safety, student conduct and technology. See [www.csba.org](http://www.csba.org).

**California Department of Education, Safe Schools:** Provides information about key elements of an effective bullying prevention program and resources to help schools recognize bullying behavior and determine how to respond, including its own comprehensive publication *Bullying at School*. See [www.cde.ca.gov/ls/ss](http://www.cde.ca.gov/ls/ss).

**Center for Safe and Responsible Internet Use:** Provides research and outreach services to address issues of the safe and responsible use of the Internet. Publications include *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats and Distress* and *Cyber-Safe Kids, Cyber-Savvy Teens*. See [www.cyberbully.org](http://www.cyberbully.org).

**Cyber Safety for Children:** This partnership between the California Office of Privacy Protection and the California Coalition on Children’s Internet Safety works toward the common goal of facilitating the safe, smart and legal use of the Internet by children. Together they provide a Web site with resources for parents, educators and community leaders and a series of educational programs for parents and educators. Coalition activities are primarily focused on keeping children safe from online predators but provide useful information about Internet safety in general as well as cyberbullying. See [www.cybersafety.ca.gov](http://www.cybersafety.ca.gov).

**Cyberbullying Research Center:** An information clearinghouse for research and publications related to cyberbullying, including order information for *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. See [www.cyberbullying.us](http://www.cyberbullying.us).

**National School Safety Center:** Offers a variety of school safety resources, including *Set Straight on Bullies* which describes myths and realities about bullying and strategies for educators. See [www.schoolsafety.us](http://www.schoolsafety.us).

**U.S. Department of Education:** The Office of Safe and Drug-Free Schools provides resources on violence prevention. See [www.ed.gov/about/offices/list/osdfs](http://www.ed.gov/about/offices/list/osdfs).

End Notes


