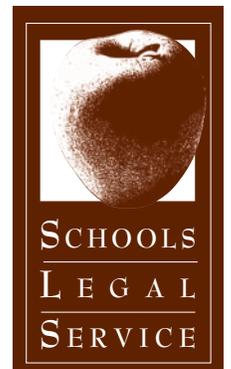




My Space or Your Space:

Internet Misconduct & Student Discipline in California Schools

by Alan B. Harris, Esq.



A CALIFORNIA ADMINISTRATOR'S GUIDE TO CYBERBULLYING AND OTHER INTERNET MISCONDUCT

*Presentation by Alan B. Harris
August 8, 2008*

The availability and widespread use of the Internet by students has inadvertently spawned a new breed of mischievous behavior and *Ferris Bueller*-type hijinks. This advisory is to alert school administrators to the issues associated with imposing discipline for student misconduct, including cyberbullying, perpetrated through the Internet. These issues involve jurisdictional challenges, due process/fair notice concerns, and free expression issues.

School districts face some significant hurdles when pursuing student discipline for Internet misconduct. Student discipline can be particularly challenging when:

- ▶ The illicit Internet activity occurs outside the jurisdictional scope of a school's discipline powers—such as after school hours, off school grounds, and/or from a privately owned computer utilizing a private Internet connection;
- ▶ The district does not have a well written “acceptable use” policy which gives fair notice that certain activities are prohibited and punishable as required by the due process guarantee in the Fourteenth Amendment to the United States Constitution; or
- ▶ The illicit Internet activity includes a communication protected by the free expression guarantees in the First Amendment, the California Constitution, and/or the Education Code. (Note that even in these circumstances, school administrators may nevertheless respond proactively by choosing a course of action from a range of nonpunitive alternatives, some of which are discussed below.)

71% of students use social networking tools at least weekly. 60% talk about education topics when on line. —NSBA: <i>Research and Guidelines on Online Social and Educational Networking.</i>
--

It is worth remembering that even if an Internet communication cannot be directly charged as misconduct, it may nevertheless be considered if it is related to another charge of misconduct. For instance, an illicit Internet communication may be used to demonstrate why seemingly innocuous conduct on school grounds may in fact be serious misconduct, such as physical intimidation.

An illicit Internet communication may also be used to prove up the secondary factual finding necessary to support an expulsion decision in the case of Education Code Section 48915(b) and (e) offenses. Specifically, Internet communications may be used to prove

that “other means of correction are not feasible or have repeatedly failed to bring about proper conduct” or that “due to the nature of the act, the presence of the pupil causes a continuing danger to the physical safety of the pupil or others.”

EXAMPLES OF INTERNET MISCONDUCT AND THE RANGE OF RESPONSES AVAILABLE TO ADMINISTRATORS

Some postings on social networking sites (MySpace, Facebook, classrooms and blogs) and some e-mail are so inappropriate that they may call for a proactive response by school administrators. Commonly known as cyberbullying, examples include communications which:

- Express a bona fide threat to the physical safety of students or staff;
- Constitute race, religion, or gender based intimidation of students or staff;
- Include personally abusive epithets which are likely to provoke a violent reaction on or around school grounds;
- Contain ideological commentary which is employed to intimidate other students;
- Are designed to incite unlawful conduct by students and actually create a “clear and present danger” of unlawful acts on school grounds;
- Deploy a fraudulent scheme designed to victimize students;
- Constitute sexual harassment;
- Constitute actionable defamation;
- Consist of “smack talk” that creates a real and substantial risk that the orderly operation of the school will be disrupted; or
- Otherwise create a poor impression of the school in the eyes of the community, such as by incorporating vulgarity, obscenity, or pornography.

Internet activity which does not involve student expression may also necessitate a proactive response. Examples include:

- Deploying invasive software, such as viruses or worms;
- Using encryption or other security measures on school systems to avoid monitoring by the school’s system administrator or school staff;
- Using a teacher’s or another student’s password without permission;
- Attempting to log onto the network as the system administrator;
- Changing files that do not belong to the user;
- Unauthorized downloading of extremely large files;
- Otherwise interfering with normal and proper operation of the school’s computers, network, e-mail system, website, or Internet access;
- Plagiarizing works found on the Internet;
- Creating a false and offensive MySpace or Facebook profile using a teacher’s likeness or identity; or

- Uploading, downloading, transmitting, or storing pornography using school equipment and/or while on the school system.

The range of proactive responses available to school administrators for addressing Internet misconduct typically includes student discipline. For example:

Cyberbullying and other Internet misconduct is typically perpetrated after school and from a home. Imposing discipline is tricky because, in this circumstance, the nexus with school activity is usually tenuous.

- Forfeiture of school computer privileges;
- Suspension;
- Expulsion;
- Involuntary transfer to continuation school (Education Code Section 48432.5);
- Imposing a community service obligation (Education Code Section 48900.6).

Non-student discipline responses are also available. These include:

- Issuing a public notice that the school is not affiliated with the expression of certain offensive ideas and disapproves of them;
- Counseling the student;
- Requiring participation in an anger management or drug and alcohol program (Education Code Section 48900(u));
- Requesting a parent to closely supervise and restrict their child’s Internet activities at home;
- Withholding grades, diplomas, or transcripts when property is damaged and restitution has not been made (Education Code Section 48904(b));
- Asking the system administrator to remove the offending material (email MySpace at schoolcare@myspace.com or call 310/969-7398; email Facebook at advertize@facebook.com);
- Filing for a civil injunction (harassment and identify theft);
- Seeking civil damages against the parents (Education Code Section 48904(a);
- Seeking a criminal complaint (Government Code section 6201– altering and falsifying a public record; Penal Code section 471 – falsifying records; Penal Code section 530.5(a) – identity theft; federal cybercrime statutes in title 18 of the United States Code).

Each listed alternative has advantages and limitations. The advantages and shortcomings of the student discipline options are highlighted below.

DISCIPLINING STUDENTS FOR INTERNET MISCONDUCT

A. Internet Misconduct Expressly Prohibited by the Education Code.

Student discipline for misconduct such as deploying worms and viruses or changing another student's files or school files is not particularly problematic. The typical charge is a violation of Education Code Section 48900(f), damaging or attempting to damage school or private property. School property includes electronic files and databases. (Education Code Section 48900(t)). Using the Internet to deploy a fraudulent or criminal scheme designed to victimize students supports a charge of violation of Education Code Section 48900(g), attempted larceny.

Remote access long after the end of the school day may create a disciplinary jurisdiction question but should not necessarily preclude prosecution. Jurisdiction exists whenever the misconduct is "related to school activity or attendance" regardless of the time of day the misconduct occurs. Education Code Section 48900(r). Although there is no California case law squarely on point, a malicious attack on the school files or a scheme to victimize fellow students should be sufficiently school related regardless of whether the attack was initiated from a site off school grounds and after the school day.

B. Internet Misconduct Not Expressly Prohibited by the Education Code.

Activity such as using encryption measures to avoid monitoring, utilizing another's password, accessing as the system administrator, downloading excessively large files, posting demeaning or defamatory information regarding staff or other students, creating a demeaning faux MySpace or Facebook profile, or transmitting/storing pornography can be problematic because these are behaviors which are not expressly prohibited by the Education Code. School administrators do not have the legal authority to discipline students unless the activity is expressly prohibited by the Education Code. Education Code Sections 48900 and 48922(b).

Fortunately, however, Education Code Section 48900(k) authorizes discipline where a student has "disrupted school activities or willfully defied the valid authority of . . . school personnel engaged in the performance of their duties." Consequently, a well drafted "acceptable use" policy could bring this sort of illicit activity within the school's disciplinary authority through the operation of Section 48900(k).

C. Acceptable Use Policies.

An acceptable use policy should make clear to students that engaging in certain activities while on a school related website, otherwise using the school's network or e-mail system, utilizing a school Internet connection, or while using school computers, cameras, or other electronic devices may result in forfeiture of school Internet and computer privileges as well as subject the offender to suspension and/or expulsion.

In order to avoid a Fourteenth Amendment/due process-fair notice issue, however, it is important that the acceptable use policy specifically, narrowly, and clearly define each type of activity that may result in disciplinary action. The school must be able to demonstrate that the offending student had prior notice of the conduct to which his/her behavior must conform. See *Flaherty v. Keystone Oaks Sch. Dist.* (W.D. PA 2003) 246 F.Supp. 2nd 698. Additionally, for each prohibited activity, it should be readily apparent that engaging in the activity would interfere with the operation of the school in a substantial way. See *Beussink v. Woodland R-IV Sch. Dist.* (E.D. MO 1998) 30 F.Supp. 1175.

Finally, in order to avoid a potential Fourth Amendment illegal search/privacy issue, the acceptable use policy should make clear that school related Internet activity may, from time to time, be monitored by school staff, and students can have no expectation of privacy. For risk management purposes, on the other hand, the policy should also make clear to parents that the scope of the school's supervision is limited to communications transmitted from school computers during school hours, that the school largely relies on the individual student complying with the acceptable use policy and on parental oversight of their own child when the child is not physically at school, and that the school will not regularly surf the Internet sites for violations but may monitor sites when alerted to a problem.

Regardless of when or where it is perpetrated, cyberbullying can harm students emotionally. These students may present a physical danger to themselves and others both during and after school activities.

D. Illicit Communications Over the Internet.

Internet activity which includes profane language, obscene expressions, sexual or other types of harassment, intimidation, outright threats of bodily injury or death, or communications advocating other students to commit unlawful acts on school grounds (aka cyberbullying and cyberstalking) may typically be charged as a violation of either Education Code Section 48900(a)(1), threatened to cause physical injury to another person, Education Code Section 48900(i), habitual profanity or vulgarity, Education Code Section 48900.2, sexual harassment, Education Code Section 48900.3, threatened to cause "hate violence," Education Code Section 48900.4, harassment, threats, or intimidation, or Education Code Section 48900.7, terroristic threats, so long as the communication is outside the ambit of constitutional free expression guarantees.

If the school's acceptable use policy contains prohibitions against such types of communications, those communications may also be prosecuted as violations of Education Code Section 48900(k), willful defiance. For example, the Education Code expressly permits schools to impose reasonable time, place, and manner restrictions on free expression. Consequently, a school's student discipline code and acceptable use policy may preclude expression that contains profanity, conveys obscene imagery, or may otherwise be lewd and vulgar. Education Code Section 48950. Such verbiage is typically outside the ambit of constitutional free expression guarantees. *Bethel Sch. Dist. v. Fraser* (1986) 478 U.S. 675.

Note that when applying the student discipline code to student expression, or drafting an acceptable use policy which precludes or regulates student expression, particular care must be taken to avoid inadvertently prohibiting communications which may be protected by the free expression guarantees of the First Amendment, the California Constitution, and the Education Code. Additionally, prior to imposing student discipline for a specific illicit communication, free expression issues must be analyzed in the particular light cast by the specific circumstances existing at the time of the communication.

E. Disciplinary Jurisdiction—Illicit Communications Made After School and at Home.

For the school to have the legal authority (jurisdiction) to impose discipline, the student misconduct must be school related. Education Code Section 48900(r). In other words, there must be a nexus between the misconduct and school activity. Consequently, student misconduct which occurs after school hours, at a student's home, and utilizing privately owned property is typically (but not always) beyond the school's disciplinary jurisdiction.

The limited scope of a school's jurisdiction does not necessarily preclude it from disciplining a student for illicit Internet communications even though those communications may originate from home, on a non-school computer and Internet connection, and late in the evening or on a weekend. For example:

When responding to cyberbullying school officials may not trample on students' First Amendment rights.
--

- An Internet communication directed at students or staff which contains sexual harassment is school related if it is severe or pervasive enough so it may be considered by a reasonable person of the same gender as the victim to create an intimidating, hostile, or offensive educational environment, or if it has had a negative impact on the victim's academic performance. (Education Code Section 48900.2)
- An intimidating or harassing Internet communication directed at students or staff is school related if it is severe or pervasive enough to create an intimidating or hostile educational environment and has the actual and reasonably expected effect of materially disrupting class work, creating substantial disorder, and/or invading the rights of students or staff. (Education Code Section 48900.4)
- An Internet communication containing a terroristic threat is school related if it has the actual and reasonably expected effect of causing students or staff to be in fear for their safety or the safety of their families, or for the protection of school or private property. (Education Code Section 48900.7.)

F. Illicit Communications and Free Speech Protection.

Assuming the necessary jurisdiction requirement is satisfied, what types of student expression on the Internet can be prohibited and/or the subject of student discipline,

censored, or otherwise punished? The applicable guidelines, unfortunately, are not particularly harmonious or consistent. Whether or not a particular communication may be prohibited and/or punished can be difficult to determine with certainty.

Guidelines codified by the Education Code are:

1. The free expression rights of students in high schools are coextensive with the rights of adults in other settings. In other words, generally, the full range of free expression guarantees which apply to adults in a non-school environment also apply, in their entirety, to communications by high school students, even in the context of a school environment (Education Code Section 48950(a)).
2. Student expression is subject to reasonable time, place, and manner restrictions (Education Code Section 48950(f)). A school publications code, outlining the responsibilities of student journalists and editors and holding them to professional standards of English and journalism, is an example of such a restriction (Education Code Section 48907).
3. Students may be disciplined for threats, harassment, and intimidation unless such illicit expression is, under the pertinent circumstances, constitutionally protected (Education Code Section 48950(d)).
4. Illicit expression, such as obscene, libelous, or slanderous communications, can be prohibited, unless otherwise constitutionally protected (Education Code Section 48907). Perhaps an example would be a political satire or parody directed at a current, controversial event where the accompanying obscenity or slander is an integral part of and inseparable from the legitimate political commentary contained in the expression.
5. Illicit expression designed to incite students to violate school rules or to commit unlawful acts on school grounds can be prohibited, provided that under the circumstances there is a clear and present danger that students will actually commit unlawful acts on school grounds, violate school regulations, or create a substantial disruption of the orderly operation of the school (Education Code Section 48907).

Guidelines are contained in case law as well. Applying case law, however, involves varying degrees of interpretation and extrapolation.

Case law guidelines include:

1. As a general rule, content based restrictions are prohibited. An Internet communication which is solely an expression of an ideological philosophy, a religious belief, or a position on a political or social issue is generally protected expression even when those ideas are communicated in an insensitive or demeaning manner. *Watts v. United States* (1969) 394 U.S. 705.

Internet speech, even when crude, juvenile and profane, in all likelihood cannot be disciplined except in limited circumstances.

2. Student expression may not be prohibited or punished, simply because the recipients may be inclined to retaliate in a physical way during school hours on school grounds. A school may not prohibit student expression simply because it presents a controversial idea and opponents are likely to cause disruption. *Smith v. Novato Unified School Dist.* (2007)150 Cal.App.4th 1439.
3. Student expression may not be restrained solely because of the desire of school administrators to avoid the discomfort and unpleasantness that may accompany an unpopular viewpoint. *Tinker v. Des Moines Indep. Cmty. Sch. Dist.* (1969) 393 U.S. 503.
4. In order to restrict student expression that may disrupt school activities, the forecast of disruption must be reasonable and fact based, the disruption forecast must be substantial, and the nature of the disruption must be that it interrupts school activities, intrudes in school affairs, or the rights of others. *Tinker v. Des Moines Indep. Cmty. Sch. Dist.* (1969) 393 U.S. 503.
5. Expression of a religious or political belief on a high school campus which is also a psychological attack on a core identifying personal characteristic of other students, such as their race, religion, gender, or sexuality, may be prohibited but it cannot be the subject of a suspension or expulsion. *Harper v. Poway Unified Sch. Dist.* (9th Cir. 2006) 445 F3d 1166.
6. Although controversial or offensive ideas and opinions may not be censored, expression which is inconsistent with the pedagogical mission of a school may be prohibited, including expression which is grammatically incorrect, poorly written, inadequately researched, unfairly biased or prejudiced, vulgar, profane, or unsuitable for immature audiences. *Hazelwood School Dist. v. Kuhlmeier* (1988) 484 U.S. 260.
7. Student expression at a school event may be restricted if it can be reasonably viewed as promoting illegal drug use. *Morse v. Frederick* (2007) 127 S.Ct. 2618.
8. A school may censor actionable defamation. *Leeb v. DeLong* (1988) 198 Cal.App.3rd 47;
9. A threat may be prohibited and punished only if it is 1) a direct, unambiguous, specific, and serious expression of the intent to inflict physical harm or death, 2) made by a student with the ability to carry it out, 3) reasonably induces fear of violence in the victim, 4) and is not made in jest, idle talk, or in the nature of a political argument. *Lovell v. Poway Unified Sch. Dist.* (9th Cir. 1996) 90 F.3d 367.
10. An offensive political or ideological expression may be prohibited if it utilizes symbolism or imagery, such as a burning cross, which has been historically employed as a virulent form of intimidation and is being used to intimidate students or staff. *Virginia v. Black* (2003) 538 U.S. 343.

It is important to remember that when faced with a jurisdictional, due process, or free speech issue that may preclude responding with student discipline, censorship, or another punitive option, alternative nonpunitive options should not be ignored. Typically, nonpunitive options can serve the need for a proactive response, ensuring student safety and maintaining an educational environment conducive to academic advancement.

TABLE OF OFFENSES: CYBERBULLYING

Cyberbullying is sending or posting harmful material in order to be cruel to others or engaging in other forms of social or emotional cruelty using the Internet or other digital technologies. Cyberbullying includes direct harassment and, also, indirect activities intended to damage the reputation of the individual targeted or cause interference in their relationship with others, such as posting harmful material, impersonating the targeted individual or disseminating personal information.¹

In order for a particular instance of cyberbullying to be the subject of student discipline: (1) All the elements of the Education Code offense must be present including the jurisdictional element; and (2) The expression must be outside the protection of the U.S. and California Constitutions.

	OFFENSE	EDUCATION CODE SECTION
1	A communication threatening to cause physical injury to staff or another student. (Must be connect to school activities or attendance.)	48900(a)(1)
2	Use of profane language or obscene expressions directed at staff or other students. (Must be connected to school activities or attendance.)	48900(i)
3	Communication(s) directed at students or staff which contain sexual harassment and are severe or pervasive enough so as to create an intimidating, hostile, or offensive educational environment or results in a negative impact on the victim's academic performance.	48900.2
4	Communication(s) directed at students or staff which is sufficiently intimidating or harassing so as to create an intimidating or hostile educational environment and has the actual and reasonably expected effect of materially disrupting class work, creating substantial disorder, and/or invading the rights of students or staff.	48900.4
5	Communication(s) containing a terroristic threat which has the actual and reasonably expected effect of causing students or staff to be in fear for their safety or the safety of their families, or for the protection of school or private property.	48900.7
6	Posting demeaning or defamatory information regarding staff or other students.	48900(k) In conjunction with an Acceptable Use Policy
7	Creating a demeaning faux MySpace or Facebook profile.	48900(k) In conjunction with an Acceptable Use Policy

¹*Cyberbullying Legislation and School Policies*, Nancy Willard, M.S. J.D., Center for the Safe and Responsible Use of the Internet, 2007.

**TABLE OF OFFENSES:
INTERNET MISCONDUCT OTHER THAN CYBERBULLYING**

Generally, school officials cannot impose student discipline unless the misconduct is expressly prohibited by the Education Code. However, since Education Code Section 48900(k) authorizes student discipline in cases where a student has “. . . willfully defied the valid authority of . . . school personnel engaged in the performance of their duties,” an “acceptable use” policy can bring illicit activity, which is not already addressed by the Education Code, within the disciplinary authority of school officials. The student, however, must have had prior notice of the school’s “acceptable use” policy.

	NATURE OF THE OFF CAMPUS/ AFTER SCHOOL MISCONDUCT	APPLICABLE EDUCATION CODE PROVISION FOR PURSUING STUDENT DISCIPLINE
1	Changing another student's files or school files	48900(f) In conjunction with 48900(t)
2	Damaging or attempting to damage school property such as electronic files and databases.	48900(f) In conjunction with 48900(t)
3	Using the Internet to deploy a fraudulent scheme designed to separate students from their money or property.	48900(g)
4	Successfully deploying malware such as a virus.	48900(f) In conjunction with 48900(t)
5	Using encryption measures with school hardware or on a school network to avoid monitoring school officials.	48900(k) In conjunction with Acceptable Use Policy
6	Utilizing a teacher’s or another student's password with school hardware or on a school network.	48900(k) In conjunction with an Acceptable Use Policy
7	Accessing a school network as the system administrator.	48900(k) In conjunction with an Acceptable Use Policy
8	Transmitting/storing pornography with school hardware or using a school network .	48900(k) In conjunction with an Acceptable Use Policy