STUDENT USE OF TECHNOLOGY: THE LEGAL FRAMEWORK IN CALIFORNIA

Schools Legal Service
Orange County Department of Education

February 2012

STUDENT USE OF TECHNOLOGY: THE LEGAL FRAMEWORK IN CALIFORNIA

Printed in the United States of America

Inquiries regarding permission for use of material contained in this publication should be addressed to:

Ronald D. Wenkart
General Counsel
Orange County Department of Education
200 Kalmus Drive, P.O. Box 9050
Costa Mesa, CA 92628-9050

SCHOOLS LEGAL SERVICE STAFF
Ronald D. Wenkart, General Counsel
Claire Y. Morey, Counsel
Lysa M. Saltzman, Counsel
Karen T. Meyers, Counsel
Norma Garcia, Paralegal

Student Use of Technology: The Legal Framework in California

TABLE OF CONTENTS

I. Introduction

Educators and courts are grappling with issues involving student use of technology both in and out of the classroom and the school. The use of technology has the ability to inspire and engage students and is an increasingly important part of most students' lives; the goal of this workbook is not to discourage the use of technology in schools, but to assist educators in helping students use the Internet, social media/Web 2.0, cell phones and other technologies in a responsible manner. Much of this workbook focuses on the small minority of students who will misuse such technologies, but our hope is that in providing resources for students and educators, we will assist not only in preventing student misconduct, but also in encouraging educators not to shy away from the use of technology because of liability concerns. In our opinion, legal risks to school districts can be minimized once educators and administrators have a comfort level with the various laws and principles that should guide their actions.

II. Investigating Alleged Student Misconduct

Once a district receives an allegation of student misconduct, the guiding principle is to gather facts in an objective manner. To that end, it will be important to speak with all of the individuals who may have knowledge of the events and ask open-ended questions that are designed to gather information rather than spread allegations. It also may be necessary to search the student and/or his belongings. It will be critical for the administrator who is investigating the matter to retain copies (hard copies and electronic copies, if possible, of the evidence). Our office has provided guidance on these issues in our Student Discipline Workbook.[1] We will briefly summarize here.

A. Interviewing the Student (and Others)

The California Supreme Court has held that school officials are not required to have reasonable suspicion that a school rule or law has been broken in order to detain and question a student, so long as such authority is not exercised in an arbitrary, capricious or harassing manner.[2] Administrators should detain and question students only when there is reason to do so, such as a need to maintain order and security in the schools. However, administrators are not obligated to obtain parent permission before interviewing a student, nor are they required to issue a warning to the student that information elicited will be used against them (i.e., Miranda warnings). If a minor student is released into the care of peace officers and removed from school premises, the principal or other school official must immediately notify the parent, guardian, or responsible relative of the minor.[3]

---

[1] August 2007.

[2] *In Re Randy G.*, 26 Cal.4th 556 (2001).

[3] Education Code section 48906. In addition, when a minor student has been taken into custody as a victim of suspected child abuse, the officer must notify the parent or guardian that the minor is in custody, but may refuse to disclose this location for up to 24 hours if there is a reasonable belief that disclosure would endanger the safety or disturb the custody of the minor.

B. Searches and Seizures

If an educator or administrator has a reasonable suspicion that a particular student has committed a violation of the law and/or school rules, he may search the student by ordering the student to empty his pockets, conducting a "pat down" search, or searching a student's locker, book bag, purse or cell phone.[4] However, the search must be reasonable both in its inception and in its scope. Therefore, if a student has violated the rule against having a cell phone turned on in class, it is reasonable to confiscate the phone; it is not reasonable to search the contents of the phone. On the other hand, if there is reasonable suspicion that the student has used his cell phone to sell drugs to another student, it may be reasonable to search the contents of the phone. That will depend on the specific facts available to the administrator.

In one case, a federal court in Pennsylvania held that it is not reasonable for school officials to search a student's cell phone looking for evidence that other students may have violated school rules.[5] In that case, the student was caught displaying a cell phone during school hours in violation of school rules. School officials then used the phone to call the student's friends to see if they too were violating the rule against use of cell phones during the school day. It also was alleged that school officials searched the text messages on the student's phone and discovered evidence of drug activity. The court held that while school officials had authority to seize the phone, they did not have authority to use it to call other students to try to catch them violating school rules, nor did they have authority to search the information contained in the phone.

Educators are reminded that strip searches, searches of body cavities or removal of clothing which exposes a student's underclothing, breasts, buttocks, or genitalia are prohibited by Education Code section 49050. Random searches or searches by members of the opposite sex that would embarrass students or invade their privacy should be avoided.

III. Criminal Conduct and Reports of Criminal Conduct

A. Is the Conduct Criminal?

There are three main statutes that criminalize electronic harassment: Penal Code sections 528.5, 653m and 653.2. Penal Code section 528.5 involves impersonation. It states in part:

> Any person who knowingly and without consent credibly impersonates another actual person through or on an Internet Web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person is guilty of a public offense ….

[4] *New Jersey v. T.L.O.*, 105 S.Ct. 733 (1985).
[5] *Klump v. Nazareth Area School District*, 425 F.Supp.2d 622 (E.D. Pa. 2006).

For purposes of this statute, "electronic means" shall include opening an e-mail account or an account or profile on a social networking Internet Web site in another person's name.

Penal Code section 653m involves conduct in which one individual threatens another by electronic means. It states in part:

> "(a) Every person who, with intent to annoy, telephones or makes contact by means of an electronic communication device with another and addresses to or about the other person any obscene language or addresses to the other person any threat to inflict injury to the person or property of the person addressed or any member of his or her family, is guilty of a misdemeanor….
>
> (b) Every person who, with intent to annoy or harass, makes repeated telephone calls or makes repeated contact by means of an electronic communication device, or makes any combination of calls or contact, to another person is … guilty of a misdemeanor."

Penal Code section 653.2, involves electronic communications that are likely to incite or produce unlawful action by a third party. It states:

> "Every person who, with intent to place another person in reasonable fear for his or her safety, or the safety of the other person's immediate family, by means of an electronic communication device, and without consent of the other person, and for the purpose of imminently causing that other person unwanted physical contact, injury, or harassment, by a third party, electronically distributes, publishes, e-mails, hyperlinks, or makes available for downloading, personal identifying information, including, but not limited to, a digital image of another person, or an electronic message of a harassing nature about another person, which would be likely to incite or produce that unlawful action, is guilty of a misdemeanor punishable by up to one year in a county jail, by a fine of not more than one thousand dollars ($1,000), or by both that fine and imprisonment."

Section 653.2 defines the phrase "of a harassing nature" as "a nature that a reasonable person would consider as seriously alarming, seriously annoying, seriously tormenting, or seriously terrorizing of the person and that serves no legitimate purpose."

Districts are not required to report suspected violations of these statutes to law enforcement; however, districts may choose to make such reports.

"Sexting" also may violate criminal laws to the extent it involves child pornography. Such conduct will be evaluated under Penal Code sections 311-313 ("obscene matter" and "harmful matter") and/or Penal Code sections 288.2 (harmful matter sent with intent of seduction of minor) or 288.3 (contact of minor with intent to commit sexual offense). The possible need to file a child abuse report for sexting is discussed below.

B. When is a Child Abuse Report Required?

Mandated reporters must make a report when they, in their professional capacity or within the scope of their employment, have knowledge of or observe a child whom they know or reasonably suspect has been the victim of child abuse or neglect.[6] The report should be made immediately or as soon as practicably possible. "Child abuse or neglect" includes sexual abuse, neglect, willful cruelty, or unjustifiable punishment, unlawful corporal punishment or injury, and abuse or neglect in out of home care. "Child abuse" does not include a "mutual affray between minors."[7] For purposes of "sexting," it is important to keep in mind the definition of "sexual abuse." Section 11165.1 defines sexual abuse as sexual assault or sexual exploitation.

"Sexual exploitation" refers, among other things, to conduct involving matter depicting a minor engaged in obscene acts, or any photograph in which a minor is involved in obscene sexual conduct. Under Penal Code section 311.3, "sexual conduct" includes "exhibition of the genitals or the pubic or rectal area of any person for the purpose of sexual stimulation of the viewer." Given the numerous statutes and cross references involved in this analysis, we recommend that mandated reporters seek legal advice if they have any questions as to whether a report is required.

C. When is a Police Report Required?

School districts are required to report suspected crimes to an appropriate law enforcement agency under the circumstances described in Education Code section 48902. Police reports are required for:

- Any acts of a pupil that may violate Section 245 of the Penal Code (assault with a deadly weapon or force likely to cause great bodily injury);

- Any acts of a pupil that may violate subdivision (c) or (d) of Section 48900 (offenses involving controlled substances, alcoholic beverages, intoxicants, or materials represented to be controlled substances, alcoholic beverages or intoxicants);

[6] Penal Code section 11166.
[7] Penal Code section 11165.6

- Any acts of a pupil that may involve the possession or sale of narcotics or a controlled substance;

- Any acts of a pupil that may involve a violation of Section 626.9 (possession of a firearm in a school zone) or 626.10 of the Penal Code (bringing or possessing weapons, as defined, on school grounds);

- A pupil or nonpupil who possesses, sells, or otherwise furnishes a firearm on a school site; and

- A pupil or nonpupil who possesses an explosive on a school site.

Absent from the above list are any "cyberbullying" or "cyberharassing" behaviors; thus, while school administrators may report such conduct to the police, they are not required to do so. The decision whether to report such conduct will depend on the egregiousness of the conduct and other factors, such as the ages of the accused and the victim.

IV. Student Discipline

A. Is the Speech Protected as "Free Speech?"

All discussions involving student speech begin with the First Amendment: "Congress shall make no law … abridging the freedom of speech."[8] As state actors, public schools are bound by this constraint both in regard to employees and to students. Further, with regard to students, schools are guided by Education Code section 48907, which states:

> "Pupils of the public schools shall have the right to exercise freedom of speech and of the press … except that expression shall be prohibited which is obscene, libelous, or slanderous. Also prohibited shall be material that so incites pupils 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."

The right to "free speech" is not absolute. Several categories of speech are unprotected, including the following:

- **Obscenity.** This is material that, taken as a whole, to the average person applying contemporary statewide standards, appeals to the prurient interest, and that, taken as a whole, depicts or describes sexual conduct in a patently

[8] U.S. Const., amend. I.

offensive way, and that, taken as a whole, lacks serious literary, artistic, political, or scientific value.[9]

- **Defamatory Material.** This requires a good faith and objectively rational determination that the speech contains a false statement, or one that cannot be proved to be true, likely to harm the reputation of another or hold that person up to shame, ridicule or humiliation. An expression of opinion is protected by the First Amendment and is not defamation.[10]

- **True threats.** A true threat exists when a reasonable person who is the object of the statement would feel threatened.[11] It is not necessary in all cases that the threat be made directly to the victim; a court may find that "in this digital age, a reasonable person could foresee the transmittal of Internet communications."[12]

- **Sexual harassment**. This term is defined in Education Code section 48900.2.

- **Harassment, threats and intimidation.** These terms are defined in Education Code section 48900.4.

- **Disruptive Speech.** This is speech that would materially and substantially interfere with the requirements of appropriate discipline in the school as set forth by the United States Supreme Court in *Tinker v. Des Moines*.[13]

This last category of unprotected speech provides considerable room for disagreement. In fact, at this point, predicting the outcome of a particular case requires the drawing of some very fine lines – lines that a court may or may not draw in the same place as a school administrator. While the cases are not all in accord, it is important to examine some of the holdings because school officials do have to make decisions as to whether speech is protected and, at this point, these cases are the best guidance there is.

In a small number of cases, the courts have found out-of-school student speech (cyberspeech) to be unprotected and have upheld the school's imposition of discipline:

- *Mardis v. Hannibal Public School District*, 684 F.Supp.2d 1114 (E.D. Mo. 2010). The student was suspended for sending an instant message to a classmate from home stating that he was going to get a gun and kill certain classmates.

[9] Penal Code section 311(a).
[10] Civil Code sections 44-46.
[11] *Lovell v. Poway Unified*, 394 F.3d 367 (9th Cir. 1996).
[12] *See Mardis v. Hannibal Public School District*, 684 F.Supp.2d 1114, 1120 (E.D. Mo. 2010).
[13] *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969).

- *Doninger v. Niehoff*, 527 F.3d 41 (2d Cir. 2008). The student was barred from running for class secretary because she posted a blog from home using lewd language to criticize school officials.

- *Wisniewski v. Board of Education*, 494 F.3d 34 (2d Cir. 2007). The student was disciplined for a drawing that shows a pistol firing at a person's head with the caption, "Kill Mr. VanderMolen." [Mr. VanderMolen was the student's teacher.]

- *J.S. v. Bethlehem Area School District*, 569 Pa. 638 (Pa. 2002). The student was disciplined for creating a website suggesting the student's teacher should die and asking for contributions to help pay the hitman.

In the majority of cases, courts have found that school administrators overreached in disciplining a student for cyberspeech. The following examples are instructive:

- *J.S. v. Blue Mountain School District*, ___ F.3d ___ (3rd Cir. 2011). The court held the district violated the student's First Amendment rights when it suspended her for creating a MySpace page purporting to be that of her school principal. The page, which she created at home, contained crude content and vulgar language suggesting the principal engaged in sexual activities in his office and made sexual advances toward students and parents. The page was accessed by other students but not at school.

- *Layshock v. Hermitage School District,* ___ F.3d ___ (3rd Cir. 2011). The court held the district violated the student's First Amendment rights when it suspended him for creating a MySpace page purporting to be that of his school principal. The page, which he created at his grandmother's house, states that the principal is a "big steroid freak" and "smoked a big blunt." The page also contains comments of a sexual nature. Although students viewed the page from a school computer on two occasions, the court did not find this to be disruptive under the *Tinker* standard.

- *J.C. v. Beverly Hills Unified School District*, 711 F.Supp.2d 1094 (C.D. Cal. 2010). The court held the district violated the student's rights when it disciplined her for posting on YouTube a video she made at a local restaurant after school. The video showed other students making derogatory and vulgar remarks about another student and was viewed by a number of students once it was posted on YouTube.

- *Killion v. Franklin Regional School District*, 136 F.Supp.2d 446 (W.D. Pa. 2001). The court held the district violated the student's rights when it disciplined him for his "top 10" list regarding the Athletic Director, including reference to the size of the Athletic Director's genitals.

- *Mahaffey v. Aldrich*, 236 F.Supp.2d 779 (E.D. Mich. 2002). The court held the district violated the student's rights when it disciplined him for his website that lists, "People I wish would die" and instructs readers to kill someone. The site contained a disclaimer warning readers not to "go out and kill and blame it on the site."

- *Coy v. Board of Education*, 205 F.Supp.2d 791 (N.D. Ohio 2002). The court held the district violated the student's rights when it disciplined him for a website referring to other students as "losers" and describing one boy as being sexually aroused by his mother.

- *Emmett v. Kent School District*, 92 F.Supp.2d 1088 (W.D. Wa. 2000). The court held the district violated the student's rights when it disciplined him for his website containing mock obituaries of his friends and asking viewers to vote on who would "die" next for purposes of the mock obituaries.

In these cases, the courts determined that the district had not established the student's out-of-school speech substantially disrupted school activities under the *Tinker* standard. Given the different approaches taken by courts in this area, we would advise school districts to seek advice from counsel prior to disciplining a student for cyberspeech.

B. Does the School Have Jurisdiction to Suspend or Expel?

Assuming that speech or other conduct is not constitutionally protected, the next question is whether the school district has jurisdiction to discipline the student for the conduct. The "free speech" analysis and the jurisdiction inquiry may overlap in some cases, but it is important to have a clear understanding of the school's authority. In the past, when a student threatened another student during a non-school event, such as a party during the weekend, schools generally did not attempt to discipline the aggressor. Now that threats can be made off-campus but spread around the community (even the world!) in an instant electronically schools are considering when they have jurisdiction to take disciplinary action. By statute, districts may impose suspension or expulsion only under certain circumstances.

Education Code section 48900(s) states:

> A pupil shall not be suspended or expelled for any of the acts enumerated in this section, unless that act is related to school activity or school attendance occurring within a school under the jurisdiction of the superintendent of the school district or principal or occurring within any other school district. A pupil may be suspended or expelled for acts that are enumerated in this section and related to school activity or attendance that occur at any time, including, but not limited to, any of the following:

(1) While on school grounds.

(2) While going to or coming from school.

(3) During the lunch period whether on or off the campus.

(4) During, or while going to or coming from, a school sponsored activity.

The essential inquiry is whether the alleged misconduct is related to school activity or attendance. Thus, for a district to suspend or expel, there should be evidence establishing that the cyberspeech has negatively impacted the school community at school or a school activity. Evidence might show, for example, that administrators have had their job duties substantially altered by the need to respond to behavior on campus and/or that students have taken significant time away from their studies discussing the matter. There are no bright lines as to how much evidence is required, so districts should be cautious and should carefully document the on-campus disruption that forms the basis for asserting jurisdiction.

C. What are the Grounds to Support Suspension or Expulsion?

If the district determines the speech is not constitutionally protected and that the school has jurisdiction because the speech is school-related under Education Code section 48900(s), the district will need to determine whether the student has committed an offense under Education Code sections 48900, 48900.2, 48900.3 or 48900.4.

Education Code section 48900(r), provides that the following conduct is grounds for suspension or expulsion:

> "Engaged in an act of bullying, including, but not limited to, bullying committed by means of an electronic act, as defined in subdivisions (f) and (g) of Section 32261, directed specifically toward a pupil or school personnel."

An "electronic act" includes electronic messages, texts, sounds or images as well as the posting of messages on a social network Internet website. However, it is important to note that under Education Code section 48900(r), cyberbullying is grounds for suspension or expulsion only if the conduct constitutes sexual harassment under Section 48900.2; hate violence under Section 48900.3; or "harassment, threats, or intimidation" under Section 48900.4.

Other sections also may support a recommendation to suspend or expel, including:

- 48900 (a) ("threats to cause physical injury to another person");

- 48900 (i) ("obscene acts and habitual profanity"); and

- 48900 (k) (disrupted school activities or otherwise willfully defied the valid authority of supervisors, teachers, administrators, school officials or other school personnel engaged in the performance of their duties.").

Districts also should consult their acceptable use policy for students to determine whether the student has violated the terms of that policy; if so, the student may be charged with a violation of 48900 (k). It is important for districts to keep their acceptable use policies current as this is a rapidly changing area. Our office has drafted a sample policy and regulations for districts. (See attached.)

V. Educating Students About Cybercitizenship

A. Legal Requirements to Educate

Both federal and state law requires school districts to educate students about cybercitizenship. Districts that accept E-rate funding must educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.[14] In addition, state law requires district technology plans to include a component to educate pupils and teachers on the appropriate and ethical use of information technology in the classroom; Internet safety; avoiding plagiarism; the concept purpose, and significance of a copyright so that pupils can distinguish between lawful and unlawful online downloading; and the implications of illegal peer-to-peer network file sharing.[15]

B. Resources for Educators and Students

Staff members in OCDE Educational Technology and Media Resources are available to provide training for administrators, teachers, staff, students, and parents concerning appropriate use of technology. Additional resources are available on the OCDE Educational Technology website, http://edtech.ocde.us/Home_1603.htm. In addition, OCDE has identified numerous resources for districts, all of which are available at no cost:

For Educators:

Digital Citizenship and Creative Content: A Teacher's Guide.
http://digitalcitizenshiped.com/

[14] 47 U.S.C. 254(h)(5)(B)(iii).
[15] Education Code section 51871.5. Technology plans in place on July 1, 2008 that lack these educational components are grandfathered, but must include such components when they expire or are voluntarily replaced.

Cyber Smart Week (Newport-Mesa Unified School District)
http://web.nmusd.us/cybersmartweek

Cyber Safety for Children (State of California Office of Privacy Protection)
http://www.cybersafety.ca.gov/

For Students/Parents:

www.onguardonline.gov/topics/net-cetera.aspx

www.bullyinginfo.org

www.nsba.org/SchoolLaw/Issues/Safety/Resources

www.GetNetWise.org

www.CyberBully411.org

www.CommonSenseMedia.org

www.iKeepSafe.org

SAMPLE BOARD POLICY

and

SAMPLE ADMINISTRATIVE REGULATION

Sample Board Policy: Student Use of Technology

Computers and other electronic resources are important tools for students to use in school and in other parts of a student life. Students are expected to be good citizens in all of their communications. It is expected that students will use these resources in a responsible manner to protect their safety and the safety of others, as well as to protect the electronic resources themselves.

Definitions:
"Technology" includes computers, tablets, the Internet, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, such as iPod's, USB drives, wireless access points (routers), or any wireless communication device.
"District Technology" is that which is owned or provided by the District.
"Personal Technology" is non-District Technology.

Use of District Technology
The District provides Technology for a limited educational purpose. This means students may use these resources for classroom activities and other school-related work. Students may not use District Technology for commercial purposes; students may not offer, provide, or purchase products or services using District Technology. Students may use District Technology only for class assignments or for personal research on subjects similar to what they might study in a class or in the school library. Use for entertainment purposes or personal communication, such as personal blogging, instant messaging, on-line shopping or gaming is not allowed.

Use of Personal Technology
Use of Personal Technology may violate this Policy if the District reasonably believes the conduct or speech will cause actual, material disruption of school activities. This Policy and accompanying Administrative Regulation will provide students with guidance in order to avoid such disruption.

Privilege, not a Right
Use of District Technology is a privilege, not a right. The District may place reasonable restrictions on the material that students access through the system, and may revoke students' access to District Technology if they violate the law, District policies or regulations.

Consequences for Violation
Violations of the law or this policy may be reported to law enforcement agencies. In addition, violations of the law or this policy may result in discipline, up to and including suspension and expulsion.

No Expectation of Privacy
Students should not expect privacy in the contents of their personal files on the District's Internet system or other District Technology. All student use of District Technology will

be supervised and monitored. The District's monitoring of student Internet usage can reveal all activities students engage in using the District's Internet system.

- Maintenance and monitoring of the District's Internet system or other Technology may lead to discovery that a student has violated this Policy, or the law. An individual search will be conducted if there is reasonable suspicion that a student has violated this Policy, the District's student discipline policy, or the law.

- Parents have the right to request to see the contents of student computer files at any time.

Acceptable Use Agreement

Before students are authorized to use District Technology and/or bring personal mobile devices to school or school activities, they and their parent/guardian are required to sign and return the Acceptable Use Agreement. Parents must agree not to hold the District or its personnel responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes or negligence. Parents also will acknowledge they may be held liable for damages caused by their child's intentional misuse of District or Personal Technology.

Responsibility for Damages

Parents can be held financially responsible for any harm that results from a student's intentional misuse of District or Personal Technology.

Filtering

In compliance with the Children's Internet Protection Act, 47 U.S.C. 254, the Superintendent or designee shall ensure that all District computers with Internet access have a technology protection measure that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced.

Instruction

The District shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying and responding to cyberbullying.

Access to Social Media Sites

The District permits/does not permit students to access social media sites, such as Facebook and Myspace, at school. [Districts should select one of the above options]

References to Related Policies:

- District Technology Plan
- Student Conduct/Discipline
- Cyberbullying
- Cell Phones
- Academic Honesty
- Use of Copyrighted Materials

Sample Administrative Regulation: Student Use of Technology

Definitions:
"Technology" includes computers, tablets, the Internet, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, such as iPod's, USB drives, wireless access points (routers), or any wireless communication device.
"District Technology" is that which is owned or provided by the District.
"Personal Technology" is non-District Technology.

Access to On-line Materials
Students shall not use District Technology to access the following:

- Material that is obscene or depicts sex or nudity
- Material that depicts violence or death or promotes weapons
- Material that is designated as "adults only"
- Material that promotes the use of alcohol, tobacco or illegal drugs
- Material that promotes school cheating
- Material that advocates participation in hate groups or other potentially dangerous groups

Inadvertent Access
If students mistakenly access inappropriate information, they should immediately report this access to a teacher or school administrator. This may help protect students against a claim that they have intentionally violated this policy.

Reports to School Officials
Students should promptly disclose to a teacher or school staff any message or other materials they receive that are inappropriate or make them feel uncomfortable. Students should not delete this information unless instructed to do so by a staff member.

Personal Information
It is important for students to protect their personal contact information, which includes their full name, together with other information that would allow an individual to locate the student, including their family name, home address or location, school address or location, work address or location, or phone number.

- Using District Technology, students shall not:
  - Disclose their personal contact information
  - Disclose other people's personal contact information*

  *Students are encouraged to follow these rules in their use of their Personal Technology as well. If student use of Personal Technology causes disruption to the school community, the student may be disciplined.

Unauthorized Access/Hacking
Students shall not gain or attempt to gain unauthorized access to District Technology, or that of another individual. This includes going beyond the student's authorized access, attempting to log in through another person's account, and accessing another person's files.

Attempts to Damage Resources
Students shall not deliberately attempt to disrupt District Technology, or that of another individual. Examples include attempts to destroy or alter data, or spread computer viruses.

Unlawful Activities
Students shall not use District Technology to engage in any unlawful act, including but not limited to, arranging for a drug sale or the purchase of alcohol; engaging in criminal gang activity; threatening the safety of any person; stealing; or cheating.*

> * Students are encouraged to follow these rules in their use of their Personal Technology as well. If student use of Personal Technology causes disruption to the school community, the student may be disciplined.

Inappropriate Language
Students shall not use obscene, profane, lewd, vulgar or threatening language using District Technology. Such use of Personal Technology may violate this Policy if the District reasonably believes the conduct or speech will cause actual, material disruption of school activities.

Sexual Harassment
Students shall not use District Technology to engage in sexual harassment. (See Educ. Code 212.5). Such use of Personal Technology may violate this Policy if the District reasonably believes the conduct or speech will cause actual, material disruption of school activities.

Hate Violence
Students shall not use District Technology to engage in hate violence. (See Educ. Code 233.) Such use of Personal Technology may violate this Policy if the District reasonably believes the conduct or speech will cause actual, material disruption of school activities.

Harassment, Threats and Intimidation
Students shall not use District or Personal technology to engage in 'harassment, threats, or intimidation' directed against District personnel or students. The phrase 'harassment, threats, or intimidation' is defined in Education Code section 48900.4.

Cyberbullying
Students shall not engage in cyberbullying, which is bullying by means of an electronic act. Cyberbullying using District Technology is prohibited, as is Cyberbullying using Personal Technology when the District reasonably believes the conduct or speech will

cause actual, material disruption of school activities. The term 'Cyberbullying' will not be interpreted in a way that would infringe upon a student's right to engage in legally protected speech or conduct. All students or others who experience, witness or become aware of cyberbullying shall immediately report it to a teacher or District administrator.

"Bullying" means any severe or pervasive physical or verbal act or conduct, including communications made in writing or by means of an electronic act, and including one or more acts committed by a pupil or group of pupils as defined in Education Code section 48900.2, 48900.3, or 48900.4, directed toward one or more pupils that has or can be reasonably predicted to have the effect of one or more of the following:

(a) Placing a reasonable pupil or pupils in fear of harm to that pupil's or those pupils' person or property.

(b) Causing a reasonable pupil to experience a substantially detrimental effect on his or her physical or mental health.

(c) Causing a reasonable pupil to experience substantial interference with his or her academic performance.

(d) Causing a reasonable pupil to experience substantial interference with his or her ability to participate in or benefit from the services, activities, or privileges provided by a school.

While not an exhaustive list, examples of cyberbullying might include:

- threats to harm another person
- written assaults, such as teasing or name-calling
- social isolation or manipulation
- posting harassing messages, direct threats, social cruelty or other harmful texts, sounds or images on the Internet, including social networking sites
- posting or sharing false or defamatory information about another person
- posting or sharing information about another person that is private
- pretending to be another person on a social networking site or other electronic communication in order to damage that person's reputation or friendships
- posting or sharing photographs of other people without their permission
- breaking into another person's account
- spreading hurtful or demeaning materials created by another person(e.g., forwarding offensive e-mails or text messages)
- retaliating against someone for complaining that they have been bullied

"Electronic act" means the transmission of a communication, including, but not limited to, a message, text, sound, or image, or a post on a social network Internet Web site, by means of an electronic device, including, but not limited to, a telephone, wireless telephone, or other wireless communication device, computer or pager.

"Reasonable pupil" means a pupil, including, but not limited to, an exceptional needs pupil, who exercises average care, skill, and judgment in conduct for a person of his or her age, or for a person of his or her age with his or her exceptional needs.

The District prohibits all bullying, including but not limited to, discrimination, harassment, intimidation and bullying based on the actual or perceived characteristics set forth in Penal Code section 422.55 and Education Code section 220, and disability, gender, gender identity, gender expression, nationality, race or ethnicity, religion, sexual orientation, or association with a person or group with one or more of these actual or perceived characteristics. In addition, the District prohibits retaliation against complainants.

Obscene Photographs

Students may not send, share, view or possess pictures, text messages, e-mails or other material of an obscene nature in electronic or any other form on Personal Technology at school or school-related activities, or using District Technology.

Mobile Devices

A. Personal Mobile Devices

The use of personal mobile devices, such as laptops, cellular phones, tablets, pagers, or other electronic signaling devices, by students on campus is subject to all applicable District policies and regulations concerning technology use, as well as the following rules and understandings:

- Permission to have a mobile device at school is contingent on parent/guardian permission in the form of a signed copy of the District's Technology Use policy and administrative regulation, except as required by Education Code section 48901.5(b).
- The District accepts no financial responsibility for damage, loss or theft. The student should keep the device in a locker when not in use. Devices should not be left unattended.
- All costs for data plans and fees associated with mobile devices are the responsibility of the student. The District does not require the use of personal mobile devices and does not rely on personal devices in its instructional program or extracurricular activities.
- Mobile devices with Internet access capabilities will access the Internet only through the school's filtered network while on school property.
- Use during class time must be authorized by the teacher.
- Photographs and audio or video recordings may be taken/made only with the express permission of all individuals being photographed or recorded. Recordings made in a classroom require the advance permission of the teacher and the school principal.

- Students may not take, possess or share obscene photographs or videos.
- Students may not photograph, videotape or otherwise record teacher-prepared materials, such as tests.
- The District will monitor all Internet or intranet access.
- If the District has reasonable cause the student has violated the law or District policy, the device may be searched by authorized personnel and/or law enforcement may be contacted.

B. District-Owned Mobile Devices

When a student is using a District-owned mobile device, all of the above rules pertaining to personal mobile devices apply as well as the following:

- The device may be used only for school-related purposes.
- Users may not download applications ("apps") to the device without permission from the teacher or other District employee.
- Users must follow all "apps" use agreements.
- The student and parent/guardian will be responsible for the replacement cost if the device is lost or is damaged because of intentional misuse.

<u>Academic Dishonesty</u>

Electronic resources can make academic dishonesty easier and more tempting for students. Students are reminded that academic dishonesty includes the following:

A. Cheating

1. Copying work from others.
2. Communicating exam answers with other students during an examination.
3. Offering another person's work as one's own.
4. Sharing answers for a take-home examination or assignment unless specifically authorized by the instructor.
5. Tampering with an examination after it has been corrected, then returning it for more credit.
6. Using unauthorized materials, prepared answers, written notes or concealed information during an examination.
7. Allowing others to do the research and writing of an assigned paper (including use of the services of a commercial term-paper company).

B. Dishonest Conduct

1. Stealing or attempting to steal an examination or answer key from the instructor.

2. Changing or attempting to change academic records without proper sanction.
3. Allowing another student to copy off of one's own work during a test.

C. Plagiarism

Plagiarism is intellectual theft. It means use of the intellectual creations of another without proper attribution. Plagiarism may take two main forms, which are clearly related:

1. To steal or pass off as one's own the ideas or words, images, or other creative works of another.

2. To use a creative production without crediting the source.

*Credit must be given for every direct quotation, for paraphrasing or summarizing a work (in whole, or in part, in one's own words), and for information which is not common knowledge.

D. Collusion

Any student who knowingly or intentionally helps another student perform any of the above acts of cheating or plagiarism is subject to discipline for academic dishonesty.

Copyrights

Students may not inappropriately reproduce or share a work that is protected by copyright. Students may not quote extensively from any source without proper attribution and permission.

Students may not make or share copies of copyrighted software, songs or albums, digital images, movies or other artistic works unless explicitly permitted by fair use provisions of copyright law. Unlawful peer-to-peer network file sharing may be a criminal offense.

System Security

Students are responsible for their individual District account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should students provide their password to another person. Students shall immediately notify a teacher or administrator if they identify a possible security problem.

Resource Limits

Students shall not download large files without permission of a teacher or administrator. Students shall not misuse District or school distribution lists or discussion groups by sending irrelevant messages.

Violations of this Policy

The District will cooperate fully with local, state, or federal officials in any investigation related to any unlawful activities. In the event that there is a claim that a student has violated the law, this Policy, or the District's discipline policy, the student's access to District Technology may be terminated, permission to bring personal mobile devices to school or school activities may be revoked, and/or the student may be disciplined under the discipline policy.