SB 178 AND STUDENT CELL PHONES

THE CONCERN

The authority to regulate possession or use of cell phones is given to Districts or their appointees by Education Code Section 48901.5(a). A District, however, may not prohibit the use of cell phones or other "electronic signaling" devices where it is "*determined by a licensed physician and surgeon to be essential for the health of the pupil and [its] use . . . is limited to purposes related to the health of the pupil*." Historically, some Districts' policies contained broad statements warning students that they have no privacy expectations with respect to cell phones and justifying intrusive searches of such devices. Such unlimited search policies are unconstitutional[1]; students have privacy rights that must be respected on campus.

Recognizing this, on January 1, 2016, SB 178, **The Electronic Communications Privacy Act**, became law (see **Attachment A**). Its purpose is to "*protect [the] personal information of all Californians*" by requiring government entities to obtain a search warrant to search and review information from smartphones and other electronic devices. The bill defines an "electronic device" as a device that stores, generates, or transmits information in electronic form (e.g. cell phones, smart phones, tablets, laptop computers, home computers, etc.). SB 178 includes strict provisions on government entities, including Districts, when attempting to obtain information directly from an electronic device or from a cell phone carrier.

Districts can now ONLY access digital information through physical interaction with an electronic device, or electronic communication with that device, under the following circumstances:

1. Pursuant to a search warrant.[2]

---

[1] New Jersey v. T.L.O. reaffirmed that students have legitimate privacy expectations in public schools. The U.S. Supreme Court ruled that any searches of students or their property need to be 1) justified from the beginning and 2) "*reasonably related [in scope] to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infractio*n." The California Supreme Court has similarly held that an administrator must have reasonable suspicion, which he/she is able to put into words; "curiosity, rumor or hunch" are not sufficient grounds to search a student (In re William G., 40 Cal. 3d 550, 564 (1985)).

[2] In the event the District is presented with a search warrant, please contact the District's legal counsel. The District, unless it has sworn law enforcement officers among its employees who shall conduct the search, should not conduct a search under a search warrant. The District should cooperate with law enforcement and follow other instructions as directed by its legal counsel. Placing a phone in "airplane mode" is considered a search. In the event a phone is frozen or

2. Pursuant to a wiretap order.[3]
3. With specific consent of the authorized possessor[4] of the device.
4. With specific consent of the owner of the device when the device has been reported stolen.
5. Exigent circumstances[5].
6. Only when the District, in good faith, believes the device to be lost, stolen, or abandoned, provided that the District only searches the device in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.[6]

---

seized, it should be placed in a "Faraday bag;" a bag designed to prevent an electronic device from being remotely wiped. In cases where a search warrant is written for a specific location, if electronic devices are located, the District will need a piggy-back warrant specifically identifying the electronic devices to be searched and the justification for the search. This is true even when generic language regarding electronic devices is included in the original warrant.

[3] In the event the District is presented with a wiretap order, please contact the District's legal counsel. The District, unless it has sworn law enforcement officers among its employees who shall conduct the search, should not conduct a wiretap under a wiretap order. The District should cooperate with law enforcement and follow other instructions as directed by its legal counsel.

[4] SB 178 defines "authorized possessor" as "the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device." It further defines "electronic device information" as "any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device." As such, a District **cannot** search a device it owns if the person holding the device is an authorized possessor except as defined within The Electronic Communications Privacy Act.

[5] An **exigency** justifying a warrantless search is **any emergency involving danger of death or serious physical injury to any person**. Any search of an electronic device conducted under the exigency exception must be followed within three days by a search warrant signed by a judge that *post facto* authorizes the already conducted search. The court shall immediately rule on the warrant. If it is determined by the judge that the search was not justified by the exigency, all data obtained from that search shall be destroyed. Searches for phones can also include emergency pings. (An emergency ping includes attempting to locate an at-risk missing person, a kidnapping victim, or a violent crime in progress by transmission of intermittent geo-coordinates.) Exigent searches of this type may be conducted by contacting the carrier of the cell phone but the justification for the exigency must be specific. It has yet to be determined how the courts will view any evidence that is located as a result of an emergency ping. A warrant or court order (once again, this is the jurisdiction of law enforcement only) will need to be completed within 72 hours of the ping. The ping and its justification will need to be thoroughly documented.

[6] There is no provision under the law to fully search a cell phone that has been 'abandoned,' other than to determine or verify the owner. Any information that is observed during the course of the search for owner information may not be used as further probable cause to extend the current search but it may be used as probable cause to support a search warrant. Absent a court ordered extension, SB 178 requires that notification to the target of the device occur contemporaneously with execution of a search warrant. Notification can be made to the owner or authorized possessor of the device by registered first class mail, email, or other reasonable means and provide the following (1) A notice that informs the recipient of the target of the investigation, (2) all information regarding the target that has been obtained, (3) the nature of the investigation under which the information is being sought and (4) a written statement setting forth the facts with necessitated the

All searches must fall under one of the six (6) sections noted above.

This hot topic addresses the impact of SB 178 on Districts effective January 1, 2016.

PROCEDURES RELATED TO USE, SEARCH, AND SEIZURE OF STUDENT CELL PHONES & RELATED DEVICES ON CAMPUSES

See **Attachment B** for a sample Board Policy that outlines appropriate use, search, and seizure guidelines related to student cell phone and other electronic signaling device use on District campuses and grounds.

HOW CAN ASCIP ASSIST YOUR DISTRICT?

If you need additional help, please contact ASCIP's Risk Services staff at (562) 404-8029 to discuss your risk management or loss control needs!

emergency. Ninety day extensions can be obtained through the courts to delay this notification process. The notification process can occur at the time of the search and must be documented.

ATTACHMENT A
SAMPLE BOARD POLICY

BP 5131.2

Student Cellular or Wireless Digital Phones and Other Personal Electronic Signaling Devices ("Permitted Devices"): Use, Confiscation, and Searches

The Governing Board believes that all students have the right to be educated in a positive learning environment free from disruptions. On school grounds and at school activities, students shall be expected to exhibit appropriate conduct that does not infringe upon the rights of others or interfere with the school program. Students may possess or use **cellular or wireless digital phones or other personal electronic signaling devices** (hereafter in this board policy, referred to as "**permitted devices**") on school campuses or grounds and at school activities except as delineated in this Board Policy.

Possession of Permitted Devices

No student shall be prohibited from possessing or using a permitted device that is determined by a licensed physician or surgeon to be essential for the student's health and the use of which is limited to health-related purposes (Education Code 48901.5). The physician's or surgeon's documentation of the health related purpose shall be presented to the principal and shall be maintained on file in the main office at the school site.

Subject to the District's guidelines, students may possess or use permitted devices on school campuses or grounds. Permitted devices shall:

1. Not be prevented from use by any student in the event of an emergency, except if such use inhibits the ability of District employees to communicate instructions related to the safety of students.
2. Not disrupt District educational programs or school activities.
3. Not be used for illegal or unethical activities such as, but not limited to, cheating on assignments or tests, cyberbullying, or sexting.
4. Not be used to record with their camera, video, or voice recording functions in ways or under circumstances which infringe upon the privacy rights of other students, District employees, or others.

5. Be turned off and kept out of sight during class time or at any other time as directed by a District employee, except for permitted devices of those specific students whose use has been deemed medically necessary or otherwise permitted by the District.

Search of Permitted Devices

Permitted devices may **not** be searched by the District, except under limited circumstances, in accordance with the limitations imposed by state and federal law. Specifically, District employees may not search permitted devices, including, but not limited to, the accessing and reading of their text messages and digital photos, **unless** those employees

1. Have the specific, written consent of the student and his or her parents or guardians,
2. Believe that an emergency involving danger of death or serious physical injury to any person (i.e., an exigent circumstance) exists,
3. Believes, in good faith, the permitted device to be lost, stolen, or abandoned and searches the device only in order to attempt to identify, verify, or contact the owner or authorized possessor of the device, or
4. Are sworn law enforcement and have orders to search the permitted device pursuant to a search warrant or wiretap order,

Student Progressive Discipline related to Permitted Devices

Violations of this policy shall be subject to progressive discipline. If a student's use of a permitted device causes a disruption, a District employee on the first offense may direct the student to turn off the device or reprimand the student. On subsequent offenses, the employee may confiscate the device (***only*** after it has been shut down by the student), and return it to the student at the end of the class period, school day, or activity. Confiscated permitted devices shall be stored by District employees in a secure manner. A student's right to carry such devices may be revoked for subsequent offenses (except where deemed medically necessary). Students may be subject to other disciplinary measures when their use of a permitted device violates independent school rules, such as prohibitions on cheating.

Responsibility for Personal Property

Students are responsible for permitted devices (and any other personal property) they bring to school. District shall not be responsible for loss, theft, or destruction of any such permitted device (or its accessories or content) brought onto school property or grounds, except that it shall be the responsibility of the District to ensure the safekeeping of any confiscated devices.

Notification

Students and their parents shall be notified of the above policy at the beginning of every school year.

Legal Reference:

EDUCATION CODE
35181 Governing board policy on responsibilities of students
35291-35291.5 Rules
44807 Duty concerning conduct of students
48900-48925 Suspension or expulsion, especially:
48908 Duties of students
51512 Prohibition use of electronic listening or recording device in classroom without permission

CIVIL CODE
1714.1 Liability of parents and guardians for willful misconduct of minor

PENAL CODE
417.25-417.27 Laser scope
647 Use of camera or other instrument to invade person's privacy; misdemeanor
647.7 Use of camera or other instrument to invade person's privacy; punishment
1546. The Electronic Communications Privacy Act

CODE OF REGULATIONS, TITLE 5
300-307 Duties of pupils

UNITED STATES CODE, TITLE 42
2000h-2000h6 Title IX, 1972 Education Act Amendments

COURT DECISIONS
Emmett v. Kent School District No. 415, (2000) 92 F.Supp. 1088
Bethel School District No. 403 v. Fraser, (1986) 478 U.S. 675
Tinker v. Des Moines Independent Community School District, (1969) 393 U.S. 503

Management Resources:

CSBA PUBLICATIONS

Cyberbullying: Policy Considerations for Boards, Governance and Policy Services Policy Brief, July 2007

Protecting Our Schools: Governing Board Strategies to Combat School Violence, 1999

CALIFORNIA DEPARTMENT OF EDUCATION PUBLICATIONS

Bullying at School, 2003

NATIONAL SCHOOL BOARDS ASSOCIATION PUBLICATIONS

Digital Discipline: Off-Campus Student Conduct, the First Amendment and Web Sites, School Law in Review, 2001

NATIONAL SCHOOL SAFETY CENTER PUBLICATIONS

Set Straight on Bullies,1989

U.S. DEPARTMENT OF EDUCATION PUBLICATIONS

Preventing Bullying: A Manual for Schools and Communities, 1998

WEB SITES

CSBA: http://www.csba.org

California Coalition for Children's Internet Safety: http://www.cybersafety.ca.gov

California Department of Education, Safe Schools Office: http://www.cde.ca.gov/ls/ss

Center for Safe and Responsible Internet Use: http://csriu.org and http://cyberbully.org

National School Boards Association: http://www.nsba.org

National School Safety Center: http://www.schoolsafety.us

U.S. Department of Education: http://www.ed.gov

U.S. Office of Juvenile Justice and Delinquency Prevention: http://www.ojjdp.ncjrs.org

Policy _____ SCHOOL DISTRICT

Adopted: _____