**Students’ Cell Phones and Electronic Devices on Campus** **BP ####**

Why is a Board Policy on Student Cell Phones Important?

Most California school districts allow school administrators to search of student cell phones if there is “reasonable suspicion” that the student violated a school rule or law – but the law has changed, and student cell phones can only legally be searched if there’s a warrant. *This is an important change, and most school and district administrators are unaware of the change*. Cell phones contain a *lot* of personal information, and there is a significant risk that a school principal’s search for information in the phone will invade the student’s privacy rights. The consequences can be very serious when the search of a student’s cell phone reveals unrelated information that is then handed over to police or anyone else. This policy is important to protect students’ privacy rights and constitutional right to be free from unlawful search and seizure.

= Required Legal Standard

= Calls for Administrative Regulation or Relies on Different Board Policy

= ACLU Identified as Most Important



| Paragraph Number | Provision | Model Board Policy | Explanation |
| --- | --- | --- | --- |
| 1–3 | **Possession and Use of Personal Electronic Devices on School Grounds** | “Students may possess or use personal electronic devices, including cell phones, on school campus provided that such devices do not disrupt the educational program or school activity and are not used for illegal or unethical activities such as cheating on assignments or tests.  Electronic devices shall be turned off and kept out of sight during class time or at any other time as directed by a school district employee, except where deemed medically necessary or when otherwise permitted by the teacher or administration. No student shall be prevented from using his/her cell phone in case of an emergency, except where that use inhibits the ability of school district employees to effectively communicate instructions for student safety.  No student shall use an electronic device with camera, video, or voice recording function in a way or under circumstances which infringe the legal privacy rights of other students.” | A board policy must explain in detail what students are and are not allowed to do with their cell phones in school, so that students do not get confused and unintentionally violate the policy. This makes the line between acceptable and unacceptable conduct clear for school officials, as well. |
| 4 | **Discipline for Cell Phone Policy Violations** | “Violations of this policy shall be subject to progressive discipline. If a student’s use of an electronic device violates this policy, a school 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 and return it to the student at the end of the class period, school day, or activity. 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 an electronic device violates independent school rules, such as prohibitions on cheating.” | School administrators, and not school police, should have exclusive responsibility for disciplining students for violating the cell phone policy. Progressive disciplinary procedures are also important to ensure that students understand the importance of the violation, and also to protect students’ right to reasonable accommodation in case of a medical necessity. |
| 5 | **Personal Electronic Devices Searches** | “Pursuant to the California Electronic Communication Privacy Act, school administrators may only search an individual student’s cell phone or electronic device with the consent of the student, pursuant to a search warrant issued by a magistrate judge based on probable cause to believe the phone contains evidence of criminal activity, or pursuant to a good faith belief that an emergency involving threat of death or serious physical injury exists that requires an immediate search of the device.” | California Electronic Communication Privacy Act (“CalECPA”) changed the standard for student cell phone searches to better protect students’ privacy rights in school. Before CalECPA was passed into law, school staff could search student cell phones if they had a reasonablesuspicion that the search would reveal evidence that the student violated a school rule or law. Now, school staff must have consent from the student to search the phone, a warrant to search the phone, or a good faith belief that an emergency involving threat of death or serious bodily injury exists that requires an immediate search of the phone. It is no longer legal for school staff to search a student’s cell phone based only on “reasonable suspicion” that the student violated a law or school rule. |
| 6 | **Personal Electronic Devices Searches—With a Warrant** | “In conducting any search of a student’s personal device pursuant to a search warrant, school staff shall: (1) document the individualized facts that supported the finding of probable cause; (2) notify the student and the student’s parent or legal guardian of the particular suspected criminal activity and the type of data to be searched for as evidence; and (3) provide the student’s parent or legal guardian the opportunity to be present during the search. In conducting any search of a student’s personal device pursuant to a good faith belief that an emergency exists, school staff shall, no later than 72 hours after accessing the device, provide to the student, the student’s parent or legal guardian, and the principal’s office: (1) a written description of the emergency, including the facts that supported the good faith belief that an emergency required an immediate search of the device; and (2) a description of the search conducted, including a summary of the data accessed and/or seized when the device was searched.” | Board policies should describe the required procedures during a search so that everyone understands them.  A search warrant must include the individualized facts that support “probable cause” to search the student’s phone. The first requirement listed here makes certain those facts are properly documented by the school.  The second and third requirements together establish an oversight system where the student and his or her parents or guardian are made aware of the search, its purpose, and its scope -- and can hold the school or district administrator accountable if the search is done illegally. |
| 7 | **Personal Electronic Devices Searches—Without a Warrant** | “In conducting any search of a student’s personal device pursuant to a good faith belief that an emergency exists, school staff shall, no later than 72 hours after accessing the device, provide to the student, the student’s parent or legal guardian, and the principal’s office: (1) a written description of the emergency, including the facts that supported the good faith belief that an emergency required an immediate search of the device; and (2) a description of the search conducted, including a summary of the data accessed and/or seized when the device was searched.” | This section lists the exception to the warrant requirement: a good faith belief that an emergency exists. The two data collection requirements listed here are an important way to make sure that districts do not label every search an “emergency” to get out of the warrant requirement. |
| 8 | **Personal Electronic Devices Searches— Required Court Approval for Emergency Searches** | “When school staff search a student’s electronic device pursuant to a good faith belief that an emergency exists, a designated school official shall, no later than 72 hours after accessing the device, file with the appropriate court: (1) an application for a warrant or order authorizing access to the electronic data; or (2) a motion that describes with specificity the facts that gave rise to the good faith belief that an emergency required the immediate search of the device. If the court determines that the facts did not give rise to an emergency, or rejects the application or order on any other ground, a designated school official must immediately destroy all information obtained through the search.” | If a school official searches a student’s electronic device without consent or a warrant, the school must seek court approval of the search within three days of conducting the search. If the court finds that the school official should not have conducted the search, the school must destroy the information obtained. This section guarantees that school officials follow this strong legal protection. |
| 9 | **Personal Electronic Devices Searches—Access to Device’s Contents** | “In the course of conducting a search, a school official shall not copy, share, or in any way transmit any information from a student’s cell phone or electronic device, or modify or delete any information.” | This sections limits who has access to the information obtained during the search, and prohibits the person searching the phone from using the student’s device. This rule prevents unintended disclosures of the student’s personal information and communications, and stops the searcher from altering information found in the student’s device. |
| 10 | **Personal Electronic Devices Searches—Scope** | “The scope of any search shall not extend beyond that to which the student consents, that which is necessary to produce evidence of criminal activity, or that which is required in an emergency.” | This section makes clear that student information is constitutionally protected. It also limits what information the school or district administrator can look for in a student’s cell phone, to avoid “fishing expeditions” for other, unrelated information in the phone. |
| 11 | **Search Logs** | “The school principal’s office shall maintain a personal device access log in which the following information shall be recorded for each search of a student’s personal device by school staff or other public employees: the name of the school official or other public employee accessing the device; the business address and other contact information for the person accessing the device; the date of access; the data or functions accessed; and the basis for the search. The log shall include documentation of searches undertaken in emergencies. Personal device access logs maintained pursuant to this provision shall not contain any personally identifiable student data, shall be made available to members of the public upon request, and shall be public records subject to the public records law.” | When school staff have to document the searches, they are almost always more careful to follow proper search procedures. This is a way to hold them accountable if an improper search is done.  This section also states that the log is a public record, so that interested community members can check to see if the correct procedures are being followed and hold “bad actors” accountable.  Personal identifying student data is confidential by law. Requiring that personal identifying information is redacted protects students’ privacy rights. |
| 12 | **Law Enforcement Access to Information Found During Search** | “Confiscated electronic devices, as well as information obtained from the electronic device through a search under this policy, will only be turned over to law enforcement when there is a real and immediate physical threat to student, teacher, or public safety or law enforcement requests the device or information pursuant to a warrant.” | This is important to make sure that police are only involved if there is a real physical threat to public safety. |
| 13 | **Procedure for Handling Student Electronic Devices** | “Students are responsible for cell phones or electronic devices they bring to school. The district shall not be responsible for loss, theft, or destruction of any such device brought onto school property, except that it shall be the responsibility of the school to ensure the safekeeping of any confiscated devices.” | This section is important because it helps protect students’ property rights, by making sure that there is a set procedure for handling confiscated phones. |
| 14–16 | **Training and Distribution** | “The Superintendent shall create and disseminate a policy regarding the return of confiscated electronics. Confiscated electronic devices shall be stored by school district employees in a secure manner in a centralized location. Confiscated electronic devices must be made available to the student at the end of the school day.  Students and their parents shall be notified of the above policy at the beginning of every school year. Students and their parents who transfer to the district in the middle of a school year shall be notified of the above policy within one week of the students’ enrollment.  Within 3 months of this policy’s adoption, [District] shall ensure that it is distributed to all school staff and that training is provided at least once per year. New or temporary staff who arrive during the middle of the school year shall be notified and trained on the policy within one week of their hire or assignment.” | This is important because it assigns the responsibility for training and distribution of the policy to a clearly identified person – which helps make sure the training and distribution actually happen. |